Neutral Citation Number: [2024] EWHC 36 (Pat)

Case No: HP-2021-000025 & HP-2021-000026

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
INTELLECTUAL PROPERTY LIST (ChD)
PATENTS COURT

Rolls Building, 7 Fetter Lane,
London, EC4A 1NL

Date: 15th January 2024

Before :

MR JUSTICE MELLOR

- -

Between :

(1) ABBOTT DIABETES CARE INC.
(2) ABBOTT LABORATORIES VASCULAR ENTERPRISES LP
(3) ABBOTT IRELAND
(4) ABBOTT DIABETES CARE LIMITED
(5) ABBOTT DIAGNOSTICS GMBH
(6) ABBOTT LABORATORIES LIMITED

Claimants in HP-2021-000025

and

(1) DEXCOM INCORPORATED
(2) DEXCOM INTERNATIONAL LIMITED
(3) DEXCOM OPERATING LIMITED
(4) DEXCOM (UK) DISTRIBUTION LIMITED

Defendants in HP-2021-000025

and

ABBOTT LABORATORIES LIMITED

Claimant/Part 20 Defendant in HP-2021-000026

and

DEXCOM INCORPORATED

Defendant/Part 20 Claimant in HP-2021-000026

and

DEXCOM INTERNATIONAL LIMITED

Part 20 Claimant in HP-2021-000026

and

(1) ABBOTT DIABETES CARE LIMITED
(2) ABBOTT DIABETES CARE INC.

Part 20 Defendants in HP-2021-000026

- -
- -

Daniel Alexander KC, James Abrahams KC, Michael Conway and Jennifer Dixon (instructed by **Taylor Wessing LLP**) for the **Abbott parties**
Benet Brandreth KC and David Ivison (instructed by **Bird & Bird LLP**) for the **Dexcom parties**

Hearing dates: 30th November, 2nd, 5-7th, 12th-13th December 2022

- -

Approved Judgment

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

Remote hand-down: This judgment will be handed down remotely by circulation to the parties or their representatives by email and release to The National Archives. The deemed date of hand down is 10.30 am on Monday 15th January 2024.

.....

THE HON MR JUSTICE MELLOR

Mr Justice Mellor :

INTRODUCTION 5
The Abbott patents 6
The Dexcom patents 7
The expert witnesses 7
Common general knowledge 8
Diabetes 8
CGM devices 13
Summary of CGM Devices 19
EP627 30
The Invention 32
THE SKILLED TEAM & CGK 35
CLAIMS / CONSTRUCTION 35
Claim 1 36
"Predetermined routine" 38
Nature of the "second indication" 39
Analysis 39
Claim 5 42
INFRINGEMENT 42
Abbott's case on infringement 42
Dexcom's non-infringement points 44
VALIDITY: NOVELTY & INVENTIVE STEP 46
The STS Guide 46
Claim 1 47
Abbott's arguments against anticipation 48
Bunte 49
CONCLUSIONS ON EP627 53
EP223 54
THE TECHNICAL CONTEXT OF EP223 54
THE SKILLED TEAM OF EP223 56
Composition of the skilled team 56
CGK for EP223 58
Mobile phones / health applications 58
CGM devices 58
Mobile phones 58
Installation checks 61

Regulatory considerations for medical device software 61
The Disputes on CGK 62
DISCLOSURE OF THE PATENT 68
Inventive concept 76
CLAIMS / CONSTRUCTION 77
Claim 1 77
'Safety critical application' 78
Integers 1.2(b) – (d) individually 79
Integers 1.2(b) – (d) compendiously 80
Discussion 84
Claims 7 and 9 86
INFRINGEMENT OF EP223 87
'installation check' 87
'functional check' 89
Selective enablement 91
The finding of no infringement by the Mannheim Court. 91
Claims 7 and 9 92
VALIDITY: NOVELTY 93
Gejdos 93
Introduction 93
Disclosure 93
Safety critical application? 95
Installation check 96
Functional check 97
Selective enablement 98
VALIDITY: INVENTIVE STEP 99
Lebel 99
Dexcom's case 100
Dr Palerm's evidence 101
Abbott's criticisms 102
Analysis 103
Dexcom's Gillette arguments 104
Claims 7 and 9 106
EP159 & EP539 109
Introduction 109
The EP159 / 539 Skilled Addressee 110
CGK points in dispute 111

Level of consensus on blood glucose levels for hypoglycaemia 111
Glycaemic variability 112
Alarm fatigue 112
The accuracy of CGM devices 112
The Specification(s) 113
CONSTRUCTION - claim 1 of EP159 115
CONSTRUCTION – claim 1 of EP539 116
EP539 Amendment 117
Extension of protection 117
Clarity 118
VALIDITY 119
Introduction 119
Brauker 2007 120
Shariati 124
Alleged Obviousness 126
Applicable principles – Inventive Step 126
Dexcom's hindsight case 129
STS-7 Guide 131
Disclosure 131
Obviousness of a predictive fixed alert 131
Navigator Guide 133
Disclosure 133
Obviousness of a fixed predictive alert 133
Other features of the claims 134
EP159, integer 1(d) – temperature correction 134
EP539, integer 1(h) – different outputs for indicators 134
EP539, integers 1(k)-1(l), visual target range 134
Dexcom's arguments against obviousness 135
Insufficiency 136
OVERALL CONCLUSIONS 136

INTRODUCTION

1. This is my judgment from Trial A in these proceedings, the first of three trials concerning various patents owned by Abbott and by Dexcom which have application in the field of Continuous Glucose Monitoring (CGM) devices. Originally there were five patents in issue for this trial, but shortly before trial Abbott withdrew its allegation of infringement of EP625, leaving four patents in issue, two owned by Abbott, EP627 and EP223 and two owned by Dexcom EP159 and EP539. Some prior art citations

were also abandoned in the lead up to trial, but at trial, there remained 9 prior art citations to consider, as well as other validity attacks.

2. CGM devices are used by diabetic patients for the purpose of monitoring their blood glucose, with a view to taking action if their blood glucose becomes too high (hyperglycaemia – requiring an injection of insulin) or too low (hypoglycaemia – requiring consumption of carbohydrate). The patents which are in issue in this trial relate, broadly, to features which involve providing users with information about their blood glucose levels and certain other characteristics. The exception is EP223 which relates to a method of checking that the application that operates on the device is installed and functioning properly.

3. There are only a handful of companies in the world involved in making CGM devices of the kind in issue. Abbott and Dexcom are the leading ones. Each has various CGM devices which it sells or proposes to sell in the UK. In the case of Dexcom, the products in issue are the G6, G7 and Dexcom ONE ("D1") systems. These are similar in several respects. In the case of Abbott, the products in issue are the FreeStyle Libre 2 ("FSL2") and FreeStyle Libre 3 ("FSL3").

4. The basic technology for these products is similar and none of the patents relate to the core functionality: they are largely features or options for the user interfaces. Here I introduce each of the patents in order of their priority dates, none of which are challenged. I analyse the issues on each patent in turn below. In general, I have addressed relevant authorities in the context of the patent where the principle issue arose (e.g. obviousness in relation to EP159), but I have kept the relevant principles in mind throughout.

The Abbott patents

5. EP (UK) 2 146 627 ("**EP627**") is entitled "Method and Apparatus for Providing Data Processing and Control in Medical Communication System". Its priority date is 14 April 2007 (the "2007 Priority Date").

6. This patent describes various aspects of a CGM but claims only a subset of the functionality disclosed. The inventive concept of the claims is said to be a method of notifying a patient of a glucose condition without thereby interrupting a routine being performed on a user interface, by outputting a first "gentle" or passive indication during the execution of the routine, to allow its continued use, but then also notifying the patient of the condition by providing a second more pronounced notification after the routine has completed.

7. EP627 is contended to be infringed by Dexcom's G6, G7 and D1 systems. Dexcom contends it is invalid for lack of novelty and/or inventive step, insufficiency and lack of patentable subject matter.

8. EP (UK) 2 476 223 ("**EP223**") is entitled "Methods and Articles of Manufacture for Hosting a Safety Critical Application on an Uncontrolled Data Processing Device" and has a priority date of 8 September 2009 (the "2009 Priority Date"). EP223 is contended to be infringed by the G6, G7 and D1 systems. Dexcom contends it is invalid for lack of novelty and/or inventive step and insufficiency. There is a conditional application to amend claim 1 (opposed only on the ground that it does not cure the alleged invalidity).

The Dexcom patents

9. EP (UK) 2 914 159 ("**EP159**") is contended to be infringed by Abbott's FSL2 and FSL3 systems. Abbott contends it is invalid for lack of novelty and inventive step, and insufficiency.

10. EP (UK) 3 782 539 ("**EP539**") is accepted to be invalid as granted. Dexcom applies to amend it: the unconditional amendment is opposed on grounds of clarity and extension of scope. If the amendment is allowed, the scope of EP539 would become materially the same as EP159 and therefore the issues, and the final result, on EP539 is accepted to be the same as for EP159.

11. The priority date of both EP159 and EP539 is 30 October 2012 (the "2012 Priority Date").

The expert witnesses

12. At the first CMC, I was inclined to and did limit the number of expert witnesses for which the parties requested permission, but at a later hearing I was persuaded to give permission for up to three experts on each side. At trial, Abbott called a single expert – Dr Cesar Palerm, and Dexcom called two – Professor Nick Oliver and Dr Vlad Stirbu.

13. Dr Palerm is an engineer who has spent the bulk of his career in the field of glucose monitoring and control. From 2004-2007, he conducted research at the University of California Santa Barbara (UCSB) including investigations using several different CGM devices including Abbott's FreeStyle Navigator device and Dexcom's STS-7. From 2007 – 2016, Dr Palerm was a Principal Scientist and later a Senior Principal Scientist at Medtronic Diabetes where he was involved in the design and product development of Medtronic's CGM devices and insulin pumps, such as the MiniMed 640G and MiniMed 670G (the first hybrid closed-loop infusion pump). From 2016-2021 Dr Palerm worked at Bigfoot Biomedical, a start-up developing a closed-loop system to regulate glucose for people with type 1 diabetes.

14. Prof Oliver is both a clinician and an engineer. He is Wynn Professor of Human Metabolism at Imperial College, London and a consultant physician in Diabetes and Endocrinology at Imperial College Healthcare NHS Trust. He has expertise in CGM design, implementation and engineering. As he explained in his first report:

> "I have been a clinician specialising in diabetes for almost 20 years. During that time, and mostly in the last 16 years, I have combined my role as a clinician with my role and work within the Department of Biomedical Engineering and the Centre for Bio- inspired Technology at Imperial College London focussing on, among other things, the development and design of CGM systems."

15. Dr Stirbu is a software engineer and consultant. For much of his career he was employed by Nokia. That work included development of remote patient monitoring by smart phone app.

16. As will appear below, in relation to all three experts, I have accepted some of their evidence and rejected other parts. Various criticisms were levelled at them and their evidence but these are best considered in context, below. Generally, I found all of their evidence informative and helpful and I am grateful to them for their assistance.

Common general knowledge

17. Although the parties prepared a single CGK Statement which identified what was agreed and disputed at all three priority dates, I prefer to separate out the CGK relating to EP223 (covering 'Mobile phone technology in 2009' and 'Regulatory considerations for medical device software') because it is self-contained and relevant only to that Patent. It is set out in the section addressing EP223 below.

18. As for the other Patents, the CGK falls into two broad categories: first, knowledge of CGM devices which existed in 2007 (for EP627) and in 2012 (for EP159 and EP539); second, knowledge of diabetes and its treatment in 2012 because it is of primary relevance to EP159 and EP539 (though much of it is background to the other Patents, even with their earlier Priority Dates). Neither expert identified any specific matters of CGK relevant to EP627 beyond knowledge of the CGM devices that existed in 2007.

19. Accordingly, what follows covers:

    i) Knowledge of diabetes and its treatment/management.

    ii) Measuring blood glucose.

    iii) Hyper- and hypoglycaemia.

    iv) Glycaemic variability in patients.

    v) CGM devices and their key features, including alarms and alerts.

    vi) The CGK as to specific CGM devices marketed from 1999 through to 2012.

20. As the parties emphasised, this is a summary of the CGK and more detail was supplied in the experts' reports.

Diabetes

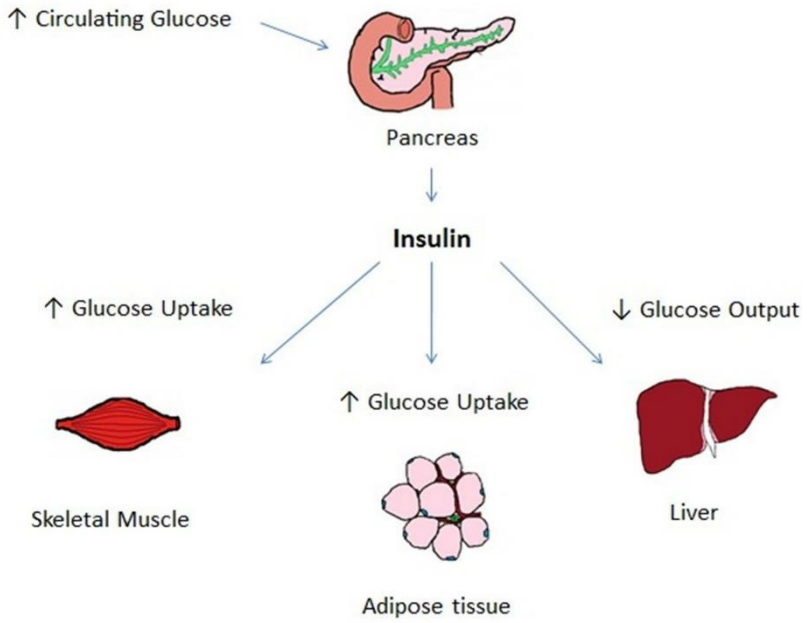
21. Unless stated otherwise, the statements made in this section constitute part of the CGK of the skilled addressee of EP159 and EP539 at the 2012 Priority Date.

Background to Diabetes

22. Glucose is the primary source of energy for the body under normal conditions. In people without diabetes, blood glucose levels are typically maintained within relatively narrow limits by the balance between glucose entry into the circulation (from stored glycogen in the liver and from intestinal absorption), and glucose uptake from the circulation into the peripheral tissues to be utilised as fuel.

23. Hormones, including insulin, maintain the balance between glucose entry into the circulation and glucose uptake by tissues, thereby ensuring glucose homeostasis.

Insulin lowers blood glucose levels by: (i) suppressing glucose output from the liver, by inhibiting both the breakdown of stored glycogen in the liver into glucose (known as glycogenolysis) and the formation of new glucose (known as gluconeogenesis); and (ii) increasing glucose uptake into peripheral tissues, by increasing the number of glucose transporter proteins at the cell surface. In people without diabetes, insulin is secreted at a low basal level throughout the day, with increased levels following mealtimes.



24. Diabetes (also called diabetes mellitus) is one of the most prevalent diseases in the world. It is a collection of chronic metabolic disorders, the characteristic feature of which is high blood glucose concentrations, resulting from an absolute or relative deficiency of insulin. People with diabetes have increased morbidity, increased risk of depression, and reduced life expectancy.

25. In 1999, the World Health Organisation ("WHO") published a new classification framework for diabetes which encompassed clinical stages and aetiological types of diabetes. It divided diabetes into the following types:

    i) Type 1 diabetes (previously known as insulin dependent diabetes);

    ii) Type 2 diabetes (previously known as non-insulin dependent diabetes);

    iii) Other specific types, including inter alia genetic defects of insulin action, genetic defects of beta cell function, diseases of the exocrine pancreas, endocrinopathies, and drug- or chemical-induced diabetes; and

    iv) Gestational diabetes.

26. In type 1 diabetes, an absolute deficiency of insulin occurs due to autoimmune destruction of the insulin-secreting beta cells of the Islets of Langerhans in the pancreas. Type 1 diabetes is generally of rapid onset, typically in childhood or adolescence (although it can occur at any age). At present, there is no cure for type 1 diabetes. As such, people with type 1 diabetes need to not only learn how to self-manage their

condition but must also maintain the motivation to self-manage their condition throughout their lifetime. The management of type 1 diabetes relies on exogenous insulin delivery (to mimic physiological insulin production as far as possible) and adherence to a group of self-care behaviours, such as estimating dietary carbohydrate and exercise. Insulin may be delivered by a regimen of multiple daily injections ("MDI") or insulin pump therapy (also known as "continuous subcutaneous insulin infusion"). The principles of self-management of type 1 diabetes are the same regardless of whether MDI or insulin pump therapy is relied on. The majority of people with diabetes rely on MDI therapy. The primary objective of type 1 diabetes self-management is to prevent immediate adverse glycaemic events; in effect constantly walking the tightrope between high glucose (hyperglycaemia) and low glucose (hypoglycaemia), as well as minimizing the risk of long-term diabetes complications.

27. In type 2 diabetes, circulating insulin cannot be utilised due to peripheral resistance to insulin at the receptor level. An insulin secretion deficit often occurs in parallel with insulin resistance. Type 2 diabetes occurs largely in adults and older people, caused by a combination of genetic and environmental factors. In the early stages of type 2 diabetes, people do not experience the extreme glycaemic variability seen in type 1 diabetes. This means that individuals can often manage their diabetes through lifestyle modification (such as weight loss through diet and exercise) as well as oral agents (tablets to either increase secretion of insulin or increase sensitivity to insulin). However, type 2 diabetes is a progressive disease. Over time, glycaemic variability increases, and the majority of people living with type 2 diabetes require exogenous insulin to manage their blood glucose levels after around 10 years, as in type 1 diabetes.

Blood Glucose Values

28. Blood glucose values are measured in units of either mg/dL or mmol/L. The unit used usually depends on the country; the preferred unit in the UK is mmol/L, whereas in the US it is mg/dL.

29. Blood glucose values may be specified as being "arterialised" (also known as "arterialised venous"), "capillary" or "venous", reflecting the type of blood vessel from which the sample was taken (arteries, capillaries, or veins respectively). At any point in time, an arterialised measurement will tend to be higher than a capillary measurement and higher again than a venous measurement. Further variability in blood glucose measurements can be introduced by measuring the glucose levels in the whole blood sample (which is typical of at-home testing) versus in the plasma component of blood only (which is typical of research settings).

30. Blood glucose values can also be estimated from measuring glucose levels in the interstitial fluid, although it should be noted that this is an estimation only due to a concentration gradient between blood and interstitial fluid, and a lag time in equilibration. The physiological lag time will vary depending on factors such as sample site and the rate of change of glucose levels. Measurement delays are also common in CGM sensors and result from filtering and processing delays in the electronic components, as well as the time required for glucose to diffuse across the outer membranes of the sensor to be in equilibrium at the enzyme layer, which can vary over time (e.g., due to biofouling or scar-tissue encapsulation of the sensor).

Hyperglycaemia

31. Hyperglycaemia, or high blood sugar, is the characteristic feature of diabetes. At the 2012 Priority Date there was no agreed definition of hyperglycaemia, but it was typically considered by most clinicians to mean a blood glucose concentration from somewhere between 10 to 15 mmol/L upwards. In the short-term, symptoms of hyperglycaemia may include feeling thirsty, peeing frequently and overnight, feeling weak or tired, and blurred vision. If untreated, hyperglycaemia can progress to diabetic ketoacidosis ("**DKA**"), a life-threatening condition requiring hospital treatment. The mainstay of treatment of DKA is insulin with supplementary fluid and supportive treatments to address electrolyte abnormalities and the underlying cause of the DKA (which may include infection as well as insulin omission). DKA predominantly occurs in type 1 diabetes where there is an absolute insulin deficiency. In developed countries, DKA has a low overall mortality rate of around <1-5% (but a much higher mortality rate in the elderly). In the medium-long term, hyperglycaemia can lead to complications of the vascular system.

Hypoglycaemia

32. Hypoglycaemia, or low blood sugar, is a serious side effect of insulin therapy. Hypoglycaemia is the leading cause of death in people with diabetes under the age of 40. It is also associated with "dead in bed" syndrome, where an individual is found dead in an undisturbed bed. For these reasons, and others, fear of hypoglycaemia is a widespread phenomenon in people with diabetes.

33. At the 2012 Priority Date, there was no universally agreed definition for all purposes of the threshold for hypoglycaemia below which a patient may be said definitively to be hypoglycaemic, although guidance and recommendations had been issued by bodies such as the European Medicines Agency (EMA) and the American Diabetes Association (ADA). However, it was universally recognised that a level of (at least) <3.0 mmol/L should be avoided and may be dangerous to at least some patients.

34. In 2002, the EMA published a "*Note for guidance on clinical investigation of medicinal products in the treatment of diabetes mellitus*". This suggested using a value of <3.0 mmol/L to define hypoglycaemia when assessing hypoglycaemic risk of new treatments for regulatory purposes.

35. In 2005, the ADA sought to define hypoglycaemia as an event accompanied by a measured plasma glucose concentration of ≤3.9 mmol/L (the "ADA Report"). The ADA Report comments that this threshold is the threshold at which glucose counter-regulation (i.e., the body's response to prevent or rapidly correct hypoglycaemia) is activated in people without diabetes, and that exposure to antecedent plasma glucose concentrations of ≤3.9 mmol/L leads to subsequent hypoglycaemic unawareness. In January 2009, a Position Statement of the American Diabetes Association recommended treating below a threshold of 70mg/dL (3.9mmol/L).

36. Around 2007, Diabetes UK, a charity aimed at patient safety, introduced the phrase "Four is the floor" suggesting people with diabetes should not let their blood glucose drop below 4 mmol/L[1].

[1] Oliver 1 ¶7.36.

37. The second edition of the Oxford Textbook of Endocrinology and Diabetes (published in July 2011) contains a chapter on hypoglycaemia. It recorded that, despite its importance, "*definitions of hypoglycaemia remain controversial*".

38. It then summarised the position on the biochemical threshold as follows:

> "Hypoglycaemia can also be defined biochemically when the blood glucose falls below a certain level. Frequency will then be dependent upon frequency of monitoring. There is no universal threshold level for defining biochemical hypoglycaemia. The use of capillary, venous, venous arterialized (sampling from a distal venous canula in a heated hand) or arterial samples will introduce variability between studies, as will the subsequent measurement of either whole blood or plasma values. Experimental studies show that evidence of cortical dysfunction can be detected in people irrespective of their recent glycaemic experience, at a plasma glucose concentration of 3 mmol/l or less (3); the original reports of the ability to induce counterregulatory deficits and loss of subjective awareness of hypoglycaemia used a 2-h antecedent exposure to 3 mmol/l (4), and early reports of the restoration of subjective awareness to the hypoglycaemia unaware by strict hypoglycaemia avoidance used avoidance of exposure to 3 mmol/l or less (5). Such data make restricting definition of hypoglycaemia to a glucose concentration of 3mmol/l or less very robust. The European Medicines Agency uses this level to define significant hypoglycaemia in assessing new medications, although pointing out that for this purpose 'the definition needs to be more rigorous than in clinical practice' (6). At the other extreme, the American Diabetes Association suggests anything less than 3.9 mmol/l be considered hypoglycaemia (2), on the basis that in health evidence of counterregulation (reduced endogenous insulin and increased glucagon secretion) is detectable at this level and artificial exposure to 3.9 mmol/l induces defects in some other aspects of the counterregulatory response to immediate subsequent hypoglycaemia in health. However, as neither insulin nor glucagon responses are useful defences against hypoglycaemia in the insulin-deficient patient with diabetes and subjective awareness to subsequent hypoglycaemia is not affected in the experimental setting just described (7), this definition, which includes glucose concentrations often seen in health, is considered by many authorities to be over rigorous, although most would acknowledge that the lower limit to goals for adjusting diabetes therapy should be at least this high. A clinically useful compromise has been to define hypoglycaemia as a plasma glucose concentration of less than 3.5 mmol/l, and certainly, in practice, this is the concentration at which patients must take corrective action. It forms a useful cut-off for defining frequency."

39. In May 2012, the EMA published its "*Guideline on clinical investigation of medicinal products in the treatment or prevention of diabetes mellitus*". It recommended that the definitions of hypoglycaemia should be standardised and stated that "*[o]ne recommended approach for such standardization is to use classifications of severity from well-accepted sources, such as the ADA for adults and ISPAD for children*" including categorising symptomatic and asymptomatic hypoglycaemia as measured plasma glucose concentrations less than or equal to 3.9 mmol/L.

Glycaemic variability

40. The management of diabetes has to be tailored to the individual with diabetes in order for it to be effective. The term "glycaemic variability" or "glucose variability" refers to the swings in blood glucose seen in people with diabetes. Each swing up or down is referred to as a glucose "excursion". These terms have been used in the field since the 1970s, such as in the metric MAGE (Mean Amplitude of Glucose Excursions). Living with diabetes means living in a state of constant flux in glucose levels requiring frequent treatment decisions (also known as "interventions"), such as injecting insulin or eating carbohydrates.

41. At a high level, swings in glucose levels can be attributed to a mismatch between the available glucose and circulating insulin. If there is more insulin than glucose, blood glucose levels will fall. The magnitude of glucose-insulin mismatch will determine the rate, and magnitude, of fall. Conversely, if there is more glucose than insulin, blood glucose levels will increase. The magnitude of the mismatch will determine the rate, and magnitude, of increase. Glucose levels are also affected by numerous other factors such as the dawn effect, caffeine, emotional responses, meals, snacking, exercise, alcohol, nocturnal hypoglycaemia, menstrual cycles, menopause, weight, fasting, illness and temperature.

42. There is also significant interpersonal variation in how blood glucose levels respond to different factors, for example if two individuals with diabetes were to eat the exact same meal, or carry out the exact same exercise routine, it will affect their glucose levels in different ways. The result is that there is no "one size fits all" approach to diabetes management.

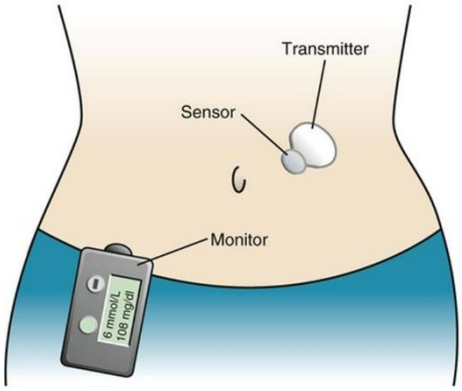
43. Individuals also have different preferences as to whether they want to maintain their blood glucose levels at the higher end of the normal range or the lower end of the normal range.

44. People also advocated for different hypoglycaemia thresholds for children. The developing brain is more susceptible to neuroglycopenia and children may be unable to express feelings or independently self-manage impending hypoglycaemia, meaning that higher hypoglycaemia thresholds for children may be more appropriate.

CGM devices

45. Unless stated otherwise, the statements made in this section constitute part of the CGK of the skilled addressee of EP627 at the 2007 Priority Date and of EP159 and EP539 at the 2012 Priority Date.

46. CGM devices provide continuous information about changes in glucose concentration in the interstitial fluid, which is present in subcutaneous tissue. CGM devices consist of a sensor, which generally remains at least partially in the subcutaneous tissue (typically the abdomen), and a monitor, which connects wirelessly via a wireless transmitter attached to the sensor, or by a cable to the sensor. The monitor may be a dedicated device or integrated into an insulin pump, or running on another device (e.g., computer).



CGM implementation

47. At the 2007 and 2012 Priority Dates, CGM implementation fell into one of two subsets:

    i) "Real-time" CGM devices, where the user would receive real-time glucose readings on their CGM monitor.

    ii) "Retrospective" CGM devices (also known as "blinded" CGM devices), where the user would have to plug their monitor into a computer and download their glucose readings from the last few days (which was typically done at the clinic). The clinician and person with diabetes would then retrospectively analyse the data. This could assist with identifying patterns in glucose levels, which could aid positive changes to treatment regimes. For example, if glucose levels were always high after lunch, the person with diabetes could modify their diet to eat less carbohydrates at lunch.

Specific CGM devices

48. A summary of CGM devices available prior to the 2007 Priority Date and the 2012 Priority Date are included in the section below.

49. All of the CGM devices available prior to the 2012 Priority Date were indicated for use as an adjunctive device only. As such, any glucose readings needed to be confirmed with a fingerprick test before an intervention was taken.

CGM glucose alarms or alerts

50. Indicators of hypoglycaemia and hyperglycaemia include notifications provided to the user, typically known as alerts and alarms. Companies use these terms differently; for example, Dexcom CGMs tend to use the term "alarm" for a more serious condition and "alert" for a less serious condition, whereas Abbott CGMs tend to use the term "alarm"

for automatic notifications that call the attention of the user to a serious condition and "alert" for notifications that will only be seen by a user actively checking their CGM display. Alarms and alerts, in general, were features of some of the earliest CGM devices and were well established as an important part of CGM devices in 2012.

51. Alarms aim to inform the patient about blood glucose concentrations outside a desired range, especially in the direction of hypoglycaemia. Such alarms may enable additional opportunities for self-management intervention and may be helpful with overnight glucose excursions which the individual may otherwise sleep through.

52. Such alarms also provide reassurance and information to the user and clinician, enabling tighter glycaemic control, particularly in patients prone to reduced or absent hypoglycaemia awareness, since they allow for prevention of, or rescue from, hypoglycaemia.

53. Glucose alerts were of three general types: (i) detection of current glucose crossing a threshold (often referred to as "current" or "threshold" alarms), and (ii) using recent glucose data with one or more algorithms to predict glucose crossing a threshold within a time period or prediction horizon (often referred to as "predictive" or "projected" alarms), and (iii) a "rate of change alert" that alerts that the user's glucose levels are rising very rapidly or falling very rapidly, regardless of the absolute value.

54. Predictive alarms are generally based on time series forecasting, which is the use of mathematical models and algorithms to forecast, predict or extrapolate future values based on past data. The aim of predictive alarms was to give the user greater warning time of a hypoglycaemic or hyperglycaemic event, thereby allowing enough time for the patient to take the necessary precautions for hypoglycaemia or hyperglycaemia mitigation and possible avoidance (e.g., consuming carbohydrates or injecting insulin). Predictive alarms were more inaccurate than threshold alarms. Shorter prediction horizons were known to increase accuracy, while longer horizons allow more time for the necessary intervention.

55. All commercially available CGM devices as of 2012 had some form of hypoglycaemia alarm. Several had multiple alarms, and combinations of current glucose alarms and predictive glucose alarms were also well known and already in use in CGM devices in 2012. The features of the CGM devices that were in use or had been released before 2012 are summarised in the next section. By way of an overview, the different types and combinations of glucose alarms in these devices is summarised in the table below, although the alarms in the devices differed in other aspects that are not captured in the table, such as how the alarms are displayed. The table refers to low glucose alarms only, although most devices also had high glucose alarms. The thresholds for the current alarms in these devices (i.e., the glucose value that triggers the alarm) could be changed by the user (i.e. "user settable" alarms) or not changed by the user (for example, factory determined, i.e. "fixed" alarms). The system set the threshold for the predictive alarms to be the same as for the current glucose alarm.

Devices	Year of release	Current alarms		Predictive alarm	
		Y/N	Fixed or user settable	Y/N	Fixed or user settable
CGK relevant to 2007 Priority Date:					
Medtronic MiniMed CGMS	1999	N	N/A	N	N/A
GlucoWatch Biographer	2002	Y	User settable Fixed at 40 mg/dL	Y	Same threshold as set by the user for the user-settable current alarm
Medtronic MiniMed Guardian RT	2005	Y	User settable	N	N/A
Medtronic Paradigm Real-Time	2006	Y	User settable	N	N/A
DexCom STS	2006	Y	(1) User settable (2) Fixed at 55 mg/dL	N	N/A
Medtronic MiniMed Guardian Real-Time	2006	Y	User settable	Y	Same threshold as set by the user for the current alarm
Additional CGK relevant to 2012 Priority Date:					
Abbott Freestyle Navigator	2007	Y	User settable	Y	Same threshold as set by the user for the current alarm
DexCom STS-7	2007	Y	(1) User settable (2) Fixed at 55 mg/dL	N	N/A
Medtronic iPro	2007	N	N/A	N	N/A
DexCom Seven Plus	2009	Y	(1) User settable (2) Fixed at 55 mg/dL	N	N/A
Medtronic iPro2	2011	N	N/A	N	N/A
Medtronic Paradigm Real-Time Revel	2010	Y	User settable	Y	Same threshold as set by the user for the current alarm
Abbott Freestyle Navigator 2	2011	Y	User settable	Y	Same threshold as set by the user for the current alarm
Dexcom G4 Platinum	2012	Y	(1) User settable (2) Fixed at	N	N/A

			55 mg/dL		

56. Of the main devices in the market as of 2012, there were two distinct approaches taken to the design of the overall alarm system exemplified by Medtronic, Abbott and Dexcom devices.

57. In the case of the Medtronic and Abbott devices, there was a single low current alarm (with one aspect being predictive) for hypoglycaemia. This threshold was user-settable. In these devices, once the user acknowledged the initial alarm, if the condition was still present sometime later (e.g., 20 minutes), the alarm would trigger again and would continue doing so until the glucose level rose above the threshold. These two systems also included predictive alarms that used a threshold set by the system to be the same as the user-settable current glucose threshold and that allowed the user to choose to get an alarm if they could be reaching this threshold in the near future.

58. In the case of Dexcom, there were two low alarms (Dexcom differentiated between these by calling one an alert and the other an alarm). The first one (the alert) was a threshold alert for hypoglycaemia with a user-settable threshold. In the Dexcom devices, once this alert was acknowledged, it would not trigger again even if the hypoglycaemic condition persisted (i.e., glucose levels must have risen above the threshold to re-set this alert). The design approach taken by Dexcom was to incorporate a second alarm with a fixed threshold at 55 mg/dL (3.1 mmol/L). This second threshold alarm thus complemented the user-settable alert. This fixed-threshold alarm was also not optional.

Display of glucose data

59. In addition to providing alarms, some CGMs could display a user's current glucose level (or most recent measured value) and historic glucose levels within a given window (typically selectable, between 1 to 24 hours). The Dexcom STS was the first CGM device to have a display able to show a graphical representation of historic glucose levels. This information was helpful for a patient to visualise trends in their glucose levels, the amount of time spent outside of target levels, and when they might be experiencing unwanted highs or lows (e.g., after meals or during exercise). In this regard, it was also known to show a user a target range alongside their actual glucose data, to allow easy visualisation of when they were (or had been) above or below a defined range. This was a feature of several CGM devices as of 2012.

Temperature correction

60. At the 2007 and 2012 Priority Dates it was known that temperature affects sensor readings and that incorporating a temperature sensor and a method to correct for it would improve the accuracy of glucose measurements in a CGM device to a degree. One reason for this is that temperature affects the rate of the enzyme-catalysed reaction, which generates the electrical signals that are ultimately converted into glucose readings. At higher temperatures, the rate of this reaction increases, so for the same amount of glucose in the reaction medium, the magnitude of the electrical current generated increases, and therefore the measured glucose value will appear to be higher.

The opposite effect may occur at lower temperatures. Another reason is that temperature can affect the rate of glucose diffusion across the sensor membrane.

Accuracy of CGM devices

61. At both the 2007 and 2012 Priority Dates, there were significant concerns over the accuracy of CGM devices.

62. In contrast to self-monitoring of blood glucose (SMBG) meters, there is no applicable ISO Standard for assessing the accuracy of CGM devices. Instead, a CGM device's accuracy can be assessed using a variety of metrics, each with their own advantages and disadvantages. Two of the most frequently used metrics for assessing the accuracy of CGM devices are the Clarke Error Grid and mean absolute relative difference (MARD).

63. The Clarke Error Grid, developed in the 1980s, was (and still is) frequently used in assessing CGM accuracy (as well as the accuracy of other glucose sensors such as fingerprick tests). The Clarke Error Grid assesses a monitor's performance on the y axis against reference glucose on the x axis, assigning a clinical risk to any glucose sensor error. Results fall into one of five risk zones:

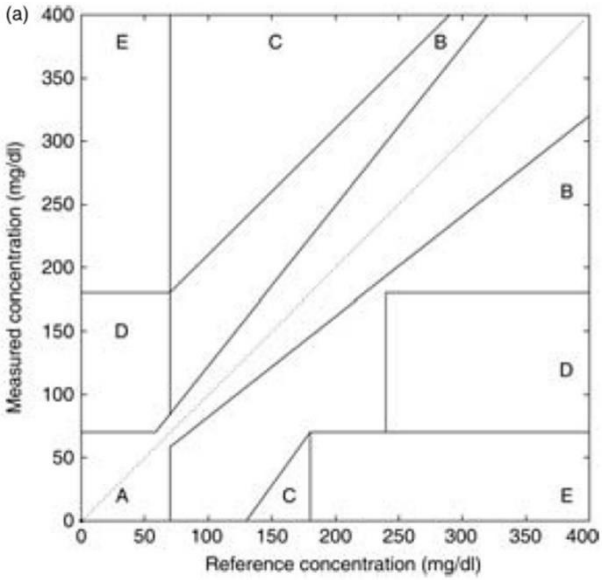
Zone A - clinically accurate;

Zone B – benign (i.e., clinically acceptable);

Zone C – overcorrect (i.e., results that may prompt overcorrection leading to hypo- or hyperglycaemia);

Zone D - failure to detect (i.e., a failure to detect hypo- or hyper-glycaemia);

Zone E - erroneous.



64. Reporting the percentage of values falling in Zones A + B of the Clarke Error Grid (representing clinically acceptable results) is a commonly used way to assess CGM accuracy; a higher percentage corresponds to higher accuracy.

65. Another way to assess accuracy was (and still is) to calculate the MARD value for a CGM device. MARD is a measure of the absolute difference between the sensor glucose value and the reference value (usually a venous blood sample), divided by the sensor glucose value and expressed as a percentage. A MARD value indicates how accurate the CGM reading of estimated blood glucose is compared against the user's real glucose value at any one time. A lower MARD value corresponds to higher accuracy.

66. The MARD value is mostly dependent on the particular CGM device being used, in particular the software algorithms, however it is also influenced by how the device is used, for example how it is calibrated as well as interference at the sensor.

Summary of CGM Devices

MiniMed CGMS (1999)

Figure A1.1: Photograph of the MiniMed CGMS

67. The MiniMed CGMS was the first CGM device to come to market, having been approved by the FDA in 1999. The MiniMed CGMS was a retrospective device that recorded glucose data for the physician to review at a later time. The user would wear the CGM device for a set period, typically for 3 days (as this was the lifetime of the sensor), and would then bring the monitor into clinic to be plugged into a computer. The clinician would then download the user's glucose data for retrospective analysis. It did not provide real-time glucose measurements to the user nor have any alerts related to glucose levels. An updated version of the device (CGMS Gold) was introduced in 2003. A further version called Guardian CGMS was released in 2004, which included high and low current glucose alarms.

GlucoWatch Biographer (2002)

Figure A1.2: Photographs of the GlucoWatch

68. The GlucoWatch Biographer was the first CGM to show real-time glucose values to the user. It launched in around 2002. Cygnus, Inc made the GlucoWatch Biographer.

69. Figure A1.2 shows the display of this device. The user could scroll through the recent measurements, and an up or down arrow presented the current trend. The glucose measurements were updated every ten minutes.

70. The GlucoWatch included three glucose alarms that would trigger if glucose readings were below the low alert level, above the high alert level, or declining towards the low alert level (down alert). The down alert was a predictive low glucose alert triggered when glucose dropped at a rate that indicated the glucose value would be below the low alert threshold within the next 20 minutes. Once any of the alarms triggered, the device would sound the alarm, repeating at periodic intervals for as long as the condition persisted. This period was 20 minutes for both the low and down (predicted low) alarms and every 40 minutes for the high alarm. The device allowed the user to set the threshold for these alerts. In addition, the GlucoWatch had a low alert for when glucose was below 40 mg/dL and a high alert for glucose values exceeding 400 mg/dL. These thresholds were fixed and corresponded to the range in which the device could read glucose values.

71. The device never gained widespread use, mainly because of accuracy issues and the discomfort it caused when taking a measurement (an electrical charge was applied to extract fluid from the skin, which was reported to cause a severe itching sensation) and was withdrawn from the market in around 2007–2008. Its FDA PMA notification was withdrawn in April 2010 (both versions). Nevertheless, as it was the first device of its kind, it would have been known to most engineers working in the field from the time it was released.

Medtronic MiniMed Guardian RT (2005)

Figure A1.3: Photographs of the Medtronic MiniMed Guardian RT

72. The MiniMed Guardian RT was the first real-time CGM system from Medtronic that presented current glucose values to the user on its display. It was released in around 2005.

73. The Guardian RT was semi-wired as the sensor had a short connecting wire to a transmitter.

74. The user could scroll through the recent measurements to get a sense of how their glucose had been changing. It did not provide any visual indication of the current glucose trend.

75. The Guardian RT had two glucose alarms: one for a sensor reading below the low threshold, the other if above the high threshold.

76. Other alarms generated by the Guardian RT were related to error conditions and included the "Check Sensor" code ("C54/CHECK"), which meant that the receiver/monitor picked up sensor current that was outside the operating range or unstable. In such a case, the User Guide advised the user to make sure the insertion site appeared normal, the sensor was still connected, and, if this error was triggered more than twice, to replace the sensor.

77. The user could turn off the low glucose alert. Its threshold could be set between 40 and 100 mg/dL (2.2 to 5.5 mmol/L). The interval at which the alert repeated defaulted to 20 minutes but could be set by the user to a longer interval of 30, 40, 50 or 60 minutes.

78. The user could also turn off the high glucose alert. Its threshold could be set between 105 and 400 mg/dL (5.8–22.2 mmol/L), with the default set at 200 mg/dL (11.1 mmol/L). As with the low glucose alert, the time interval could be set. The default was 60 minutes and could be set between 60 and 180 minutes in 30-minute increments. When the high glucose alert was on, the user had the option of "snoozing" the alert for a set period of time (between one and twelve hours); during the snooze period, the high glucose alert was deactivated.

79. The user could also choose how the device would alert: audible, vibration or both. The audio had three volume settings (low, medium and high).

Dexcom STS (2006)

Figure A1.4: Photograph of Dexcom STS

80. The STS was the first CGM device from Dexcom. It was launched in around 2006. The STS was a real-time CGM device and provided the user with glucose measurements every 5 minutes for up to 3 days (72 hours).

81. As seen in Figure A1.4, the STS showed the current glucose value together with a graph and an indication in a text (under the current glucose value) of what the time range in

the graph covered. The dotted lines shown represent the thresholds of the high and low glucose alerts.

82. The STS had three threshold glucose alerts/alarms. There was an adjustable low and high glucose threshold alert and a low glucose alarm which was not adjustable. The user could turn off the low and high glucose alerts. The low glucose alert had a default setting of 80 mg/dL (4.5 mmol/L) and could be adjusted between 60 to 90 mg/dL in increments of 10 mg/dL. The high glucose alert's default was 200 mg/dL (11.1 mmol/L) and could be adjusted in a range of 140 to 400 mg/dL in increments of 20 mg/dL. The low glucose alarm used a threshold of 55 mg/dL (3.1 mmol/L) that could not be changed, nor could the low glucose alarm be turned off.

83. The alert sequence of the STS device was the same for both the low and high glucose alerts. When the threshold was first crossed (and the trend was to go further into the alert range), the device vibrated and displayed the alert screen (including the notification "Low" or "High" and the relevant threshold level). After five minutes, if there had been no acknowledgement of the alert, the device beeped once. After another five minutes had elapsed with no acknowledgement, the device beeped again at an increased volume. The alerts were acknowledged by pressing any of the device buttons and would not re-alert once acknowledged (until the alert reset by exiting the alert condition). If the alert was not acknowledged and the alert condition remained, it would re-alert after 15 minutes.

84. For the low glucose alarm, the STS first vibrated and, after five minutes, sounded a loud beep if it had not been acknowledged. The STS continued to repeat this vibrate/beep pattern until the alarm was acknowledged. Alongside these notifications, the low glucose alarm screen was displayed, showing the word "Low" alongside the 55mg/dL threshold value. As with the two settable threshold alerts, the user acknowledged the alarm by pressing any button on the device. If the alarm condition persisted after 30 minutes, even if already acknowledged, the device would start alarming again and continue to do so until glucose levels rose above 55 mg/dL (3.1 mmol/L).

85. The STS device also displayed various silent indications related to its operation status, including missing data with "Y" antenna or a pictogram depicting the STS losing the connection with the transmitter.

86. The STS device also had a visual notification ("---" alongside the Y antenna) for when "noisy" glucose readings were received. Users receiving this notification were advised to check the placement of the STS Sensor to make sure it was still adhered to their skin properly and that nothing was rubbing the STS Sensor (i.e. clothing, seat belts). The "noisy" glucose readings could also occur due to rapid increases or decreases in the user's glucose levels.

87. The STS also had alerts to notify how much time the user had remaining until the 3-day sensor session was complete. The Expiration Screen will appear 6 hours and 2 hours before the 3-day session ends. At the 30 minute and 0 hour Expiration Screen, the STS Receiver will display the Expiration Screen and will also vibrate. The user can clear all of these screens by pressing any button on the STS Receiver. In the period prior to sensor expiration, the glucose readings are still being taken as normal. Upon expiration, the 0 hour Screen appears and no more glucose readings are read. The user then knows to remove their STS Sensor.

88. At a general level, the principle of warning users of expiry is part of any medical device design; it is considered a safety feature. The medical device should have an indication of remaining life span in order to be safe, useable and effective, whilst not interrupting its main function (which in the case of a CGM device is the measuring of the glucose level). For example, in the context of CGM devices, if a user receives an alert in the evening that their sensor will expire in 6 hours, it allows them to replace it early to ensure they have a functioning sensor overnight.

Medtronic MiniMed Guardian Real-Time (2006)

Figure A1.5: Photographs of Medtronic MiniMed Guardian Real-Time

89. The Guardian Real-Time was launched in around 2006. The Guardian Real-Time provided the user with glucose values in real time.

90. As seen in Figure A1.5, the Guardian Real-Time presented the historical glucose values in a graph (with the user being able to select between time windows of 3, 6, 12 and 24 hours). The display showed the current time and glucose value and trend arrows. The trend arrow in this device included one or two arrows to not only indicate the direction of change but the magnitude of the change (one arrow if the magnitude of the rate was 1.0–2.0 mg/dL/min; two arrows if the magnitude was 2.0 mg/dL/min or greater; no arrow if the magnitude of the rate was less than 1.0 mg/dL/min).

91. As with the STS, the dotted lines on the graph represented the thresholds of the low and high glucose alerts mentioned below.

92. The Guardian Real-Time device distinguished between an alert and an alarm. The term "alarm" was used for events/conditions affecting the system's ability to function properly. All other forms of alert were referred to as "alerts", including glucose alerts and conditions that affect how the system measures glucose levels.

93. The user could choose how all alarms/alerts are sounded. The default was a medium beep, but a long beep, short beep or vibration were other options.

94. The Guardian Real-Time device provided the following glucose alerts:

    i) Low glucose alert/high glucose alert. The thresholds for the Low and High alerts were adjustable by the user;

    ii) Predicted low and predicted high glucose alerts. The threshold level for the Low Predicted alert was whatever threshold had been set by the user for the Low alert. In effect, the Low Predicted alert was an early warning that the user's glucose level was reaching the threshold for the Low alert. The same was true

for the High Predicted and High alerts. The prediction horizons were also settable by the user;

iii) Falling and rising rate alerts.

95. By default, all glucose alerts were turned off. Once turned on, the low and high alerts provided an alert when the measured glucose value fell below or went above a threshold. There were default thresholds, but the user could adjust them. Furthermore, the device allowed different thresholds to be used during different times of day (up to eight segments), including the possibility of the alerts being turned off during some of these time segments. The defaults were also different depending on the model, with the paediatric version having more conservative default thresholds (90 mg/dL for the low alert in the paediatric version, versus 60 mg/dL for the adult version, and 280 mg/dL versus 200 mg/dL for the high alert).

96. The low glucose threshold could be set within a range of 40 to 390 mg/dL (90 to 390 mg/dL for the paediatric version). The high glucose threshold had to be at least 10 mg/dL higher than the low threshold, with a possible range of 50 to 400 mg/dL (100 to 400 mg/dL for the paediatric version).

97. The threshold for the predicted low/high glucose alerts use was the same as the threshold for the low/high alerts, but the user could configure the prediction horizon (e.g., a setting of 20 minutes meant the predictive alert would trigger when the prediction was that the glucose values would reach or exceed the threshold 20 minutes into the future). The default prediction horizon for both high and low predictive alerts was 15 minutes and could be set in a range of 5 to 30 minutes (in increments of five minutes). These settings applied to all time segments. The predictive alerts could be turned off even if the threshold alerts were on.

98. The Guardian Real-Time also included falling and rising rate alerts. As with the predictive alerts, these could be turned off even if the other glucose alerts were on, and the rise and fall alerts could also be turned on/off independent of each other. The threshold for the rate of change was the same for both (in terms of the magnitude of the rate of change), with a default of 4.0 mg/dL/min; the range was from 1.1 to 5.0 mg/dL/min.

99. All the glucose alerts continued to sound until they were cleared. They also repeated until the condition that caused the alert was resolved, even after clearing them. There were two snooze settings to regulate how often these alerts would repeat after the alert was cleared. The snooze for the high glucose alerts (high glucose, predicted high glucose and rise rate of change) defaulted to a one-hour time period but could be set between five minutes and three hours. For the low glucose alerts (low glucose, predicted low glucose and fall rate of change), the default snooze period was 20 minutes and could be set between five minutes and one hour.

100. The Guardian Real-Time also allowed the user to temporarily silence glucose alerts (they were still noted on the display and recorded in the device's log). The options were to silence only the high alerts, only the low alerts, both low and high alerts, and all sensor glucose alerts (including the low transmitter battery alert). When silencing, the user chooses how long the alerts would be silent (from 30 minutes to 24 hours).

101. Around 2006, Medtronic incorporated CGM capability into its insulin infusion pump, the MiniMed Paradigm Real-Time (the "Paradigm Real-Time"). The UI was very similar to the Guardian Real-Time, with only a few additional status indications on the screen that were specific to the insulin pump functionality. The Paradigm Real-Time had high and low glucose alerts but not predictive alerts.

102. The Guardian Real-Time also had a Sensor Error alert: the reason for the Sensor Error alert being that the sensor signal is either too high or too low. If this alert was repeated the user was instructed to "*make sure that the sensor is inserted properly, that the sensor and transmitter are connected properly, and that there is no moisture at the connection*".

103. Like all early CGM devices, the Guardian Real-Time had regulatory approval for use as an adjunctive device only. Therefore, the real time data that it was providing on glucose values or alerts could not be relied upon to make an intervention decision. Instead, the data was intended to provide an indication of when a fingerprick test may be required. This message was in the Guardian Real-Time user guide, which also strongly recommended that the user work closely with their healthcare professional when using the device.

Dexcom STS-7 (2007)

Figure A1.6: Photograph of Dexcom STS-7

104. The STS-7 was the second generation of Dexcom's CGM. It was launched in around 2007. The STS-7 expanded the use of a single sensor from three days to seven (thus the seven in the name of the device).

105. From an interface perspective, the STS-7 was very similar to the original STS. The only difference was that instead of showing the start and end time of the range covered by the graph, it showed the current time and the number of hours into the past that the graph shows.

106. The glucose alerts in the STS-7 were almost the same as in the original STS. A difference was a change in how the low and high glucose alerts were announced. In the STS-7 device, the first notification was via vibration. If not acknowledged, the second one was five minutes later and was a vibration followed by a beep. If still not acknowledged, the third one was five minutes after the second one and was a vibration

followed by two beeps. After this, the device would no longer provide vibration/audio alerts, even if the alert had not been acknowledged. The low glucose alarm had the same pattern as the high/low alerts but would start alarming again after 30 minutes if the glucose readings were still below the alarm threshold.

107. Other system alerts and notifications were also unchanged from the behaviour of the STS device.

Abbott FreeStyle Navigator (2007)

Figure A1.7: Photograph of the Abbott FreeStyle Navigator

108. The Navigator was the first CGM system from Abbott Laboratories. It was released in around 2007.

109. As seen in Figure A1.7, the main screen of the Navigator did not show a graphical representation of past glucose values. However, the user could display such a graphical representation through the report function. The Navigator included trend arrows, which indicated direction and magnitude. An arrow at a 45-degree angle (up or down) represented a magnitude between 1.0–2.0 mg/dL/min, an arrow straight up or down for a magnitude greater than 2.0 mg/dL/min, and a flat arrow pointing right if the magnitude was less than 1 mg/dL/min. When viewing their glucose level history through the reports function, the user could view a line graph of their glucose data alongside a shaded region representing a target range. This range was separate from the high and low glucose alarms discussed below.

110. The Navigator had threshold low and high glucose alarms and a projected (predictive) alarm for both high and low glucose (as with the Guardian Real-Time, the system set the threshold for the projected alarms based on the threshold settings for the low and high glucose alarms). All of these could be turned off if desired.

111. The low glucose alarm threshold defaulted to 65 mg/dL and could be set in a range between 60 and 139 mg/dL. The high glucose alarm defaulted to 300 mg/dL and could be set in a range between 140 and 300 mg/dL. The projected low and high glucose alarms could be set independently to three sensitivity levels (high sensitivity used a prediction horizon of 30 minutes, medium sensitivity used a prediction horizon of 20 minutes, and low sensitivity a prediction horizon of 10 minutes). How an alarm was

announced could be set individually for each of these alarms; the choices were a low, medium or high beep or a short, medium or long vibration.

112. The Navigator allowed the user to mute all audible alarms for one hour. For all alarms, if the display was not turned on during the first hour of notification of an alarm, the receiver would stop beeping/vibrating, and no further alarms would sound until the display had been activated.

113. Alarms were given a level of urgency based on how soon the user should respond, and alarms acted differently depending on the urgency level. A high level of urgency alarm could not be muted; the annunciation was the same as the medium urgency alarms. Medium urgency alarms could be muted; they sounded three short beeps every six seconds for one minute or until the display was activated. They repeated every five minutes until acknowledged or the condition was resolved and repeated every 15 minutes after acknowledgement until the condition was resolved. An intermediate level of urgency was the same as medium urgency, except that the intermediate alarm would stop and not sound again after one hour or after acknowledgement and could be muted. A low level of urgency was enunciated with a single beep that could be muted, and it did not repeat after acknowledgement.

Medtronic iPro (2007)

114. Medtronic released the iPro in around 2007. The iPro was the successor to Medtronic's CGMS Gold. It was another retrospective CGM device aimed at clinicians, but unlike the CGMS Gold it now had a wireless receiver. As the iPro was a retrospective CGM device, it did not have any alerts relating to glucose levels.

Dexcom Seven Plus (2009)

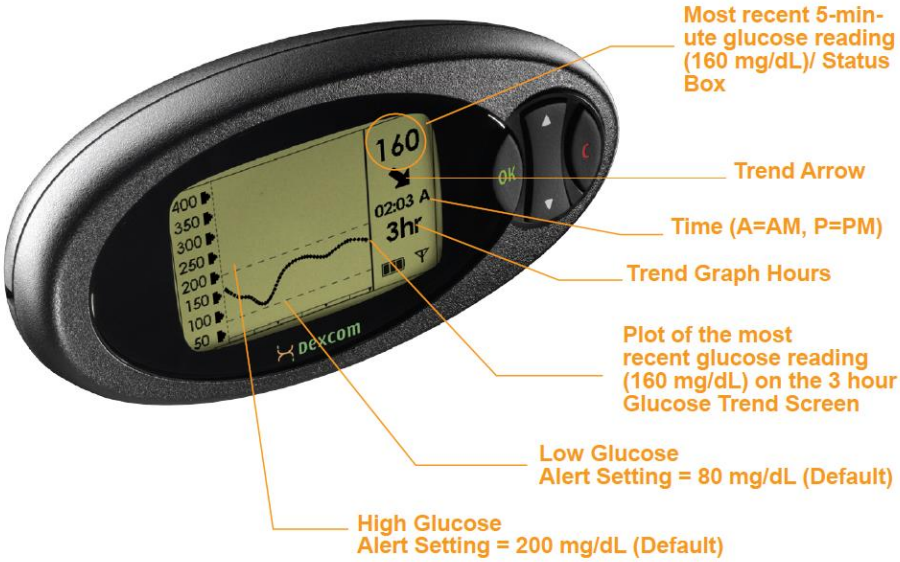


Figure A1.8: Photograph of Dexcom Seven Plus

115. This was an updated version of the STS-7, it received CE mark approval in 2009. As shown in Figure A1.8 above, it had a similar form factor to the STS-7 and STS and had very similar features.

116. As seen from Figure A1.8, the Dexcom Seven Plus (the "Seven Plus") UI displayed a graphical representation of a user's historical glucose data and a numerical indication of the user's most recent 5-minute reading. Like the STS-7, it showed the current time and the number of hours of glucose data shown as a graph of the recent glucose levels and dotted lines showing the thresholds for the low and high glucose alerts. New in the Seven Plus were the glucose trend arrows, which indicated the direction in which the user's glucose levels were heading.

117. Like the STS-7 and the STS, the Seven Plus had high and low glucose alerts, the thresholds for which were settable by the user, and a low glucose alarm, which was fixed at 55 mg/dL. In addition, the Seven Plus introduced rate-of-change alerts. These could be selected to be on or off by the user. If on, they alerted the user when their glucose levels were rising or falling more rapidly than a threshold rate. The user could choose whether to receive alerts when the rate of rising or falling was at or greater than 2 mg/dL per minute ("Rise" and "Fall" alerts) or when the rate was at or greater than 3 mg/dL per minute ("Rapid Rise" and "Rapid Fall" alerts).

118. The way the High and Low alerts, Rise and Fall/Rapid Rise and Rapid Fall alerts were indicated in the Seven Plus was slightly different from the STS-7. For each of these alerts, if activated, the user could choose between "Vibe then Beep" or "Vibrate" modes. Like the STS-7, the "Vibe then Beep" mode alerted first with a vibration only and then every 5 minutes with a vibration and audible beeps. For the High Glucose Alert and Rise Alerts, the repeat alerts were a vibration and two high tone beeps, whereas the Low Glucose Alert and Fall Alerts were indicated with a vibration and three low tone beeps. The "Vibrate" mode alerted using vibrations only. For each of these alerts, the user could also select a "snooze" function, through which they could choose whether to receive further alerts at 30 mins, 1, 2, 3, 4 or 5 hours after initially acknowledging the alert.

119. The low glucose alarm used a first vibration, then after 5 minutes, if not acknowledged, a vibration followed by four beeps, and then after a third 5 minutes, a vibration plus four louder beeps. As with the STS and the STS-7, the low glucose alarm would automatically sound again after 30 mins if the user's glucose remained at or below the threshold, even if the first alert was acknowledged. These settings could not be changed or turned off by the user.

Abbott Freestyle Navigator II (2011)

120. The FreeStyle Navigator II was released in around 2011. It was an updated version of the original FreeStyle Navigator. However, there were no changes to the glucose alerts described above between the original FreeStyle Navigator and the updated Navigator II.

Medtronic Paradigm Real-Time Revel

Figure A1.9: Photograph of Medtronic Paradigm Real-Time Revel

121. The Medtronic Paradigm Real-Time Revel (the "Paradigm Real-Time Revel") was a combined CGM and insulin pump device released by Medtronic in 2010. This device was an update to the Paradigm Real-Time device including predictive alerts and fall and rise rate alerts. The alert settings were the same as described above in relation to the Guardian Real Time.

Medtronic iPro2 (2011)

Figure A1.10: Photograph of the Medtronic iPro2

122. Medtronic released the iPro2 in around 2011. Like the iPro it was a retrospective CGM device so did not have any alerts relating to glucose levels.

Dexcom G4

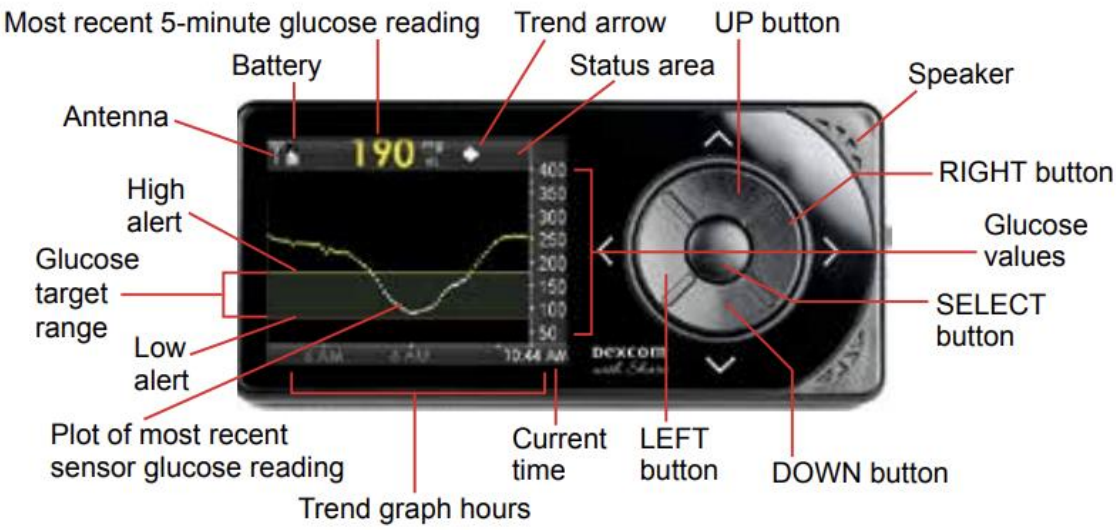


Figure A1.11: Photograph of Dexcom G4 Platinum

123. The G4 (referred to as the Dexcom G4 Platinum in the United States) received CE mark approval on or before 14 June 2012 and FDA approval on 5 October 2012. The G4's sensing technology was integrated into Johnson & Johnson's Animas Vibes insulin pump which received CE mark in June 2011, allowing patients to use the pump as an alternative to, or in conjunction with, the G4 receiver. The alarm/alert functionality of the G4 was in all material respects the same as the Seven Plus.

EP627

124. Almost all the issues which I have to decide on EP627 depend upon the correct interpretation of claim 1. Dexcom submit that the claim is expressed in deliberately broad terms and accused Abbott and their expert, Dr Palerm, of reading additional limitations into the claim which are not reflected in the language used. By contrast, Abbott submitted that Dexcom's approach ignored the context and purpose of the invention.

125. EP627 is entitled 'Method and apparatus for providing data processing and control in medical communication system'.

126. As will be seen below, the invention claimed in EP627 is described in a few short paragraphs of the specification and by reference to one of the figures. Since most of the issues in this action turn on the correct interpretation of claim 1, it is necessary to review some other parts of the specification to see if they provide any assistance.

127. The specification starts with three paragraphs under the heading 'Background'. These paragraphs start by talking about an analyte sensor but immediately address blood glucose as the analyte. After describing aspects of the sensor, which are not pertinent, the specification addresses the portion of the sensor which communicates readings to the transmitter unit which sends readings to a receiver/monitor unit where data processing takes place:

> [0002] ….

> The transmitter unit is configured to transmit the analyte levels detected by the sensor over a wireless communication link such as an RF (radio frequency) communication link to a receiver/monitor unit. The receiver/monitor unit performs data analysis, among others on the received analyte levels to generate information pertaining to the monitored analyte levels. To provide flexibility in analyte sensor manufacturing and/or design, among others, tolerance of a larger range of the analyte sensor sensitivities for processing by the transmitter unit is desirable.
>
> [0003] The state of the art is exemplified by the document US 5 791 344 A, which discloses a method comprising executing a predetermined routine associated with an operation of an analyte monitoring device; detecting a predefined alarm condition associated with the analyte monitoring device; outputting a first indication associated with the detected predefined alarm condition during the execution of the predetermined routine; and outputting a second indication associated with the detected predefined alarm condition.

128. By reference to that description of the state of the art, the invention is summarized in [0004]. It can be seen that [0003] describes the pre-characterising portion of claim 1 and [0004] describes the characterising portion:

> [0004] Relative thereto the invention is defined in claim 1. In it the second indication is output after the execution of the predetermined routine; the predetermined routine is executed without interruption during the outputting of the first indication; and the first indication includes a temporary indicator and, further, the second indication includes a predetermined alarm associated with the detected predefined alarm condition; and the predetermined routine includes one or more processes that interface with a user interface of the analyte monitoring device.

129. Neither side made reference to or suggested that the acknowledged prior art US344A assisted on the issues of construction which arise.

130. Although the Detailed Description starts with the general statement that the patent provides a method and apparatus for providing data processing and control for use in a medical telemetry system, it immediately takes as its paradigm a CGM system and indeed it states in terms:

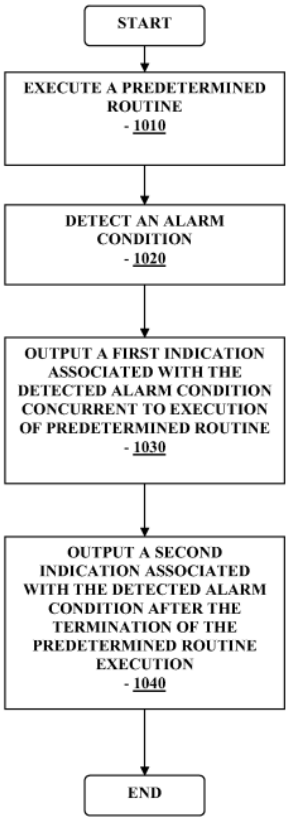
> 'The subject invention is further described primarily with respect to a glucose monitoring system for convenience and such description is in no way intended to limit the scope of the invention. It is to be understood that the analyte monitoring system may be configured to monitor a variety of analytes'.

131. A variety of analytes are set out in [0009], making it very clear that the invention applies well beyond CGM systems.

132. The specification then describes various aspects of a CGM system but none of the detail matters for present purposes.

The Invention

133. The invention is described at [0077] – [0081], by reference to figure 10 (shown below):



134. In summary, as Abbott submitted:

i) In this figure, the predetermined routine begins at box 1010 and continues until it is terminated in box 1040. Paragraph [0080] explains that the predetermined routine may include performing a finger stick blood glucose test "*or any other processes that interface with the user interface".* Several examples are given, including review of historical data such as glucose data, alarms and events, and visual displays of data. So these are routines which involve the user interacting with the user interface in some way, and are associated with analyte monitoring, but not for the monitoring itself.

ii) During execution of the predetermined routine, if an alarm condition is detected (box 1020), the user is notified by a "*first indication"* that alerts the user "*substantially in real time"* to the detected alarm condition, but *"does not interrupt or otherwise disrupt the execution of the predetermined routine*" (box 1030, [0078] – [0079]).

iii) Upon the user terminating the predetermined routine, a second indication associated with the alarm condition is output or displayed (box 1040, [0078]).

iv) The purpose of the process is that a detected alarm condition can be notified to the user immediately, but without immediately interrupting or disrupting an ongoing routine or process ([0081]).

135. Additional information regarding the first and second indications is provided at [0137] – [0152].

> '[0137] A method in accordance with still yet another embodiment may include executing a predetermined routine associated with an operation of an analyte monitoring device, detecting a predefined alarm condition associated with the analyte monitoring device, outputting a first indication associated with the detected predefined alarm condition during the execution of the predetermined routine, outputting a second indication associated with the detected predefined alarm condition after the execution of the predetermined routine, where the predetermined routine is executed without interruption during the outputting of the first indication.
>
> [0138] In one aspect, the predetermined routine may include one or more processes associated with performing a blood glucose assay, one or more configuration settings, analyte related data review or analysis, data communication routine, calibration routine, or reviewing a higher priority alarm condition notification compared to the predetermined routine, or any other process or routine that requires the user interface.
>
> [0139] Moreover, in one aspect, the first indication may include one or more of a visual, audible, or vibratory indicators.
>
> [0140] Further, the second indication may include one or more of a visual, audible, or vibratory indicators.
>
> [0141] In one aspect, the first indication may include a temporary indicator, and further, and the second indication may include a predetermined alarm associated with detected predefined alarm condition.
>
> [0142] In still another aspect, the first indication may be active during the execution of the predetermined routine, and may be inactive at the end of the predetermined routine.
>
> [0143] Further, the second indication in a further aspect may be active at the end of the predetermined routine.
>
> [0144] Moreover, each of the first indication and the second indication may include one or more of a visual text notification alert, a backlight indicator, a graphical notification, an audible notification, or a vibratory notification.

> [0145] The predetermined routine may be executed to completion without interruption.
>
> [0146] An apparatus in accordance with still another embodiment may include a user interface, and a data processing unit operatively coupled to the user interface, the data processing unit configured to execute a predetermined routine associated with an operation of an analyte monitoring device, detect a predefined alarm condition associated with the analyte monitoring device, output on the user interface a first indication associated with the detected predefined alarm condition during the execution of the predetermined routine, and output on the user interface a second indication associated with the detected predefined alarm condition after the execution of the predetermined routine, wherein the predetermined routine is executed without interruption during the out- putting of the first indication.
>
> [0147] The predetermined routine may include one or more processes associated with performing a blood glucose assay, one or more configuration settings, analyte related data review or analysis, data communication routine, calibration routine, or reviewing a higher priority alarm condition notification compared to the predetermined routine.
>
> [0148] The first indication or the second indication or both, in one aspect may include one or more of a visual, audible, or vibratory indicators output on the user interface.
>
> [0149] In addition, the first indication may include a temporary indicator, and further, wherein the second indication includes a predetermined alarm associated with detected predefined alarm condition.
>
> [0150] Also, the first indication may be output on the user interface during the execution of the predetermined routine, and is not output on the user interface at or prior to the end of the predetermined routine.
>
> [0151] Additionally, the second indication may be active at the end of the predetermined routine.
>
> [0152] In another aspect, each of the first indication and the second indication may include a respective one or more of a visual text notification alert, a backlight indicator, a graphical notification, an audible notification, or a vibratory notification, configured to output on the user interface.'

136. These paragraphs specify that the first and second indications may include one or more of a visual, audible or vibratory indicator ([0139] – [0140]), and that the first indication may include a temporary indicator ([0141]).

137. The specification therefore specifically contemplates that there will be an unobtrusive indication (which does not interrupt or otherwise disrupt) the user's use of the application and which may include a temporary indicator.

138. As will be apparent from the prior art Dexcom relies on in this case, this concept of holding back the "full" alert in favour of an unobtrusive indication, so as not to interrupt the user, and only providing the normal alert after they had completed the routine they were engaged in, was not a feature of any CGM devices. That is unsurprising, since notifying the user of a glucose condition through glucose alerts was one of the key functions of CGM devices.

THE SKILLED TEAM & CGK

139. There does not appear to be any dispute as to the core attributes of the engineer or engineers who both experts regard as the relevant skilled person/skilled team. They would be an engineer (such as a systems engineer, biomedical engineer or electrical engineer, but not necessarily from any specific engineering discipline) specialising in the design of medical devices. The engineer would have experience in CGM design, albeit their level of experience in CGM design is unlikely to affect any of the issues on EP627.

140. The only CGK of specific relevance to EP627 that either expert has identified is the skilled team's knowledge of existing CGM devices as of 2007 (see the summary of CGM devices at the Annex to the CGK Statement). This would include familiarity with their UIs and with provision/display of alarms, alerts and notifications.

CLAIMS / CONSTRUCTION

141. The principal claims in issue are claims 1 and 5 (method claims). Claims 8 and 12 are the equivalent apparatus claims, respectively, and it is not necessary to address them separately. There is no need to rehearse the applicable principles which are well-known. No issues of equivalents were raised so I must undertake a purposive construction of the claims: see e.g. *Saab Seaeye Ltd v Atlas Electronik GmbH* [2017] EWCA Civ 2175 per Floyd LJ at [18] & [19] and *Icescape Ltd v Ice-World International BV* [2018] EWCA Civ 2219 at [60].

142. By the time of closings, Abbott submitted that two issues of construction arose concerning 'predetermined routine' and (essentially) the nature of the second indication. However, as I have already indicated, most of the issues on EP627 turn on issues of construction. In the breakdown of claim 1 below, I have underlined those expressions which I consider to be in issue:

Claim 1

1	*A method comprising*
1.1	*executing, on a receiver unit (104, 106), a predetermined routine associated with an operation of an analyte monitoring device (1010);*
1.2	*detecting a predefined alarm condition associated with the analyte monitoring device (1020);*
1.3	*outputting, to a user interface of the receiver unit, a first indication associated with the detected predefined alarm condition during the execution of the predetermined routine (1030); and*
1.4	*outputting, to the user interface of the receiver unit, a second indication associated with the detected predefined alarm condition (1040);* ***wherein***
1.5	*the second indication is output after the completion of the execution of the predetermined routine;*
1.6	*the predetermined routine is executed without interruption during the outputting of the first indication;*
1.7	*the first indication includes a temporary indicator and,*
1.8	*further, the second indication includes a predetermined alarm associated with the detected predefined alarm condition; and*
1.9	*the predetermined routine includes one or more processes that interface with the user interface of the receiver unit.*

143. Before I come to the issues, I found it helpful to set out the integers of the claim by reference, first, to the stated characteristics of the predetermined routine (PDR) and, second, the chronological sequence of events, and I use this structure below:

i) The PDR is executed on the receiver unit, which has a user interface.

ii) It must be associated with an operation of an analyte monitoring device.

iii) It must include one or more processes that interface with the user interface of the receiver unit.

iv) During the execution of the PDR, a first indication is output to the user interface associated with the detected predefined alarm condition (which alarm condition is associated with the analyte monitoring device).

v) The PDR must execute without interruption during the output of the first indication.

vi) The first indication (which (as above) is associated with the detected predefined alarm condition) includes a temporary indicator.

vii) After the completion of the execution of the PDR, the second indication is output, the second indication being associated with the detected predefined alarm condition.

viii) The second indication includes a predetermined alarm associated with the detected predefined alarm condition.

Interpretation of Claim 1

144. Abbott submitted that claim 1 is a claim to the method described above by reference to figure 10. In summary:

i) The method involves the user using their CGM receiver unit in some interactive way (a "*predetermined routine*" – e.g. retrieving historical CGM data – integers 1.1, 1.9).

ii) If an alarm condition is met (integer 1.2), the user is alerted in a manner which does not interrupt the *predetermined routine* (the "*first indication*" – integers 1.3, 1.6, 1.7).

iii) Then, once the user has completed what they were doing, a second indication will be output on the receiver unit – e.g. one which the user cannot ignore (the "*second indication*" – integers 1.4, 1.5, 1.8).

145. Abbott relied on this sentence in Dr Palerm's first report: "*The aim is to ensure that the user is only momentarily disturbed while executing the routine, but once it is over, a more prominent "second indication" will appear*."

146. Abbott also stressed that <u>both</u> the "*predetermined routine*" <u>and</u> "*the alarm condition*" must be "*associated with … the analyte monitoring device*". This is true. They also submit that the invention is not about (i) suppressing alarms while the user is using some different application unrelated to the analyte monitoring device or (ii) suppressing alarms that are not related to the analyte monitoring device.

147. Abbott's submissions shared some ground with the way Dr Palerm characterised the inventive concept of EP627, and he made it clear that his discussion of EP627 was predicated on this understanding throughout:

> In summary, the inventive concept claimed in EP627 is a method of notifying <u>a patient</u> of <u>a glucose condition</u> without interrupting a routine being performed <u>on a user interface</u> by outputting a first <u>passive</u> indication during the execution of the routine, but then also <u>reminding</u> the patient of the condition by providing a second <u>more permanent</u> indication after the routine has completed.

148. Dexcom attacked this, contending it was riddled with errors:

i) The claim is not limited to notifying a patient – it simply speaks of a "user", which Dr Palerm agreed could be a parent or doctor of a patient using a CGM. In fact, the claim is not even expressly limited to medical analytes.

ii) The claim is not limited to an alarm which concerns a glucose condition (by which Dr Palerm appeared to mean hyper- or hypoglycaemia) – it refers to "an alarm condition associated with an analyte monitoring device", which:

a) is not limited to a device monitoring glucose but includes any analyte monitoring device, as Dr Palerm accepted; and

b) is not limited to alarms associated with an analyte condition (i.e. significantly high or low levels of the analyte) but includes alarms such as system errors and battery level alarms, as Dr Palerm also accepted.

iii) There is no requirement that the "predetermined routine" is performed on a user interface – the claim simply requires that the predetermined routine is "associated with an operation of an analyte monitoring device" and includes "one or more processes that interface with the user interface of the receiver unit".

iv) The degree of permanence of the second indication is not specified – it is simply necessary that it "includes a predetermined alarm associated with the detected predefined alarm condition".

149. Moving to the individual terms used in claim 1, Abbott addressed two: the PDR and 'the nature of the second indication'. I will set out Abbott's submissions and, briefly, Dexcom's response.

"Predetermined routine"

150. The additional limitations which Abbott suggested should be interpreted into this expression appear from their submissions which were as follows:

i) Paragraph [0080] describes predetermined routines in which the user is interacting with the user interface, such as "*the configuration of device settings*" and "*review of historical data such as glucose data*". Such processes are described as "*processes that interface with the user interface*". Integer 1.9 limits the claim to that sort of predetermined routine. So the "*predetermined routine*" of claim 1 is one involving the user interacting with the user interface.

ii) The word used in the claim is a "*routine*"; and integer 1.9 says that that involves one or more "*processes*". So that excludes something as simple as the standard screen display without any interaction from the user. (It is notable that Prof Oliver ignores integer 1.9 in his attempt to understand this part of the claim.)

iii) This is also clear as a matter of purposive construction. The whole point of the claim is that the routine is not immediately "*interrupted or otherwise disrupted*" while it is being executed, but instead an unobtrusive indication, including a temporary indication, is given to the user; but once complete, a second indication (an "*alarm*") is given to the user. This only makes sense if the *routine*

is one that involves the user; and thus it is desirable to alert them (integer 1.3), but not interrupt what they are doing (integer 1.6); and also to set off an "*alarm*" once they have completed the routine.

iv) The patent gives specific examples of routines which fall within that definition.

151. By contrast, Dexcom submitted that 'a predetermined routine' is deliberately broad, but acknowledged the express limitations in the claim (which I set out below).

Nature of the "second indication"

152. Abbott submitted as follows:

i) EP627 does not specify the nature of the second indication beyond defining it as a "*predetermined alarm associated with the detected alarm condition*". Nevertheless, the experts agreed as to its nature and purpose. It is to provide a more prominent or permanent notification, in contrast to the initial less obtrusive (and in particular non-disruptive) notification of the first indication. Or in Prof Oliver's terms, "*the user is then notified of the event again (in a more permanent manner)*".

ii) There was some attempt by Dexcom in Dr Palerm's cross-examination to suggest that the purpose of the second notification is no more than an additional "*reminder*". Dr Palerm does describe the second notification as having that role (and it can do so in some cases) but that is neither a limitation in the claim nor of the inventive concept as it has been understood by both experts. The point is that the second notification is more "*prominent*" or "*permanent*" in the sense that it is one that the user is required to deal with. Having had the gentle "shoulder tap" of the first indication, the user is then presented with the second notification which requires some action or acknowledgement of the alarm condition that has been detected.

Analysis

153. In reality, there is a single point underpinning the proper interpretation of claim 1. For the most part, Abbott are trying to interpret claim 1 as restrictively as possible and by reference to the embodiment described in the Patent. By contrast, Dexcom point to the obvious generality of the wording used in claim 1, but Dexcom also seek to impose limits on the claim where it suits them.

154. As Floyd J. (as he then was) explained in *Nokia v IPCom* [2009] EWHC 3482 (Pat) at [41]:

> "Where a patentee has used general language in a claim, but has described the invention by reference to a specific embodiment, it is not normally legitimate to write limitations into the claim corresponding to details of the specific embodiment, if the patentee has chosen not to do so. The specific embodiments are merely examples of what is claimed as the invention, and are often expressly, although superfluously, stated not to be 'limiting'. There is no general principle which requires the court to assume that the patentee intended to claim the most sophisticated embodiment of the invention. The skilled person understands that, in the claim, the patentee is stating the limits of the monopoly which it claims,

> not seeking to describe every detail of the manifold ways in which the invention may be put into effect."

155. With that principle in mind, I turn to consider the interpretation of various terms used in claim 1. Although they are set out in a certain order below, I emphasise that the process of interpretation is an iterative one, so that all considerations are taken into account. It is convenient to start with the elements which are somewhat in the background of the claim. I remind myself this is a method claim.

'analyte monitoring device'

156. It is clear that the monitoring device is not limited to monitoring glucose. Any analyte can be monitored.

157. There is an ability to detect a predefined alarm condition associated with the analyte monitoring device.

158. The first and the second indications are both associated with that (the same) predefined alarm condition.

'receiver unit'

159. The implication in the claim is that the analyte monitoring device communicates in some way (e.g. transmits data, including data indicating alarm conditions associated with the analyte monitoring device) to the receiver unit. Nothing turns on this, but it helps to make sense of the claim. The receiver unit has a user interface, and some sort of computer processing ability so the PDR is able to execute on the receiver unit.

160. The issue over the 'receiver unit' arises because of one of Dexcom's non-infringement arguments, but the argument confuses the distinction between the receiver unit (which has some computer processing ability) and routines which run on it.

'user interface'

161. The user interface has the ability to provide the first and second indications which are output to it. In terms of the provision of the first and second indications, the user interface could be very simple - for example the first and second indications could be indicated to the user via individual lights. It could (but need not) be a screen.

162. However, it is important to note that there are one or more processes in the PDR which interface with the user interface, the implication being that there is some output from the PDR on the user interface. So the user interface has (at least) a dual role.

163. It seems to me that apart from having these functional requirements, the receiver unit and its characteristics (including its user interface) are expressed in deliberately general terms.

'predetermined routine'

164. The claim requires the PDR:

i) to execute on the receiver unit.

ii) to be associated with an operation of an analyte monitoring device.

iii) to include one or more processes that interface with the user interface of the receiver unit.

iv) to execute without interruption during the output of the first indication.

v) to complete execution (before the output of the second indication).

165. At this point, I simply note that in the infringement case the second indication is caused by the user ending the routine by tapping the notification.

'first indication'

166. The claim requires the first indication:

i) to be associated with the detected predefined alarm condition (which alarm condition is associated with the analyte monitoring device).

ii) to be output to the user interface during the execution of the PDR.

iii) to include a temporary indicator.

167. It is implicit that the output of the first indication must end before the second indication is output to the user interface.

'second indication'

168. The claim requires the second indication:

i) to be associated with the detected predefined alarm condition (which alarm condition is associated with the analyte monitoring device).

ii) to be output to the user interface after the completion of the execution of the PDR.

iii) to include a predetermined alarm associated with the detected predefined alarm condition.

169. The issue over the second indication stems from one of Dexcom's non-infringement arguments. Dexcom submit that the second indication must be a reminder, but this is not a requirement of the claim.

Conclusions

170. I realise that in these paragraphs I have done little more than restate the express wording from the claim, but this exercise of setting out what is required of each element in the claim serves to highlight where the parties (but mostly Abbott) seek illegitimately to write in additional limitations.

171. Whilst it is essential to take account of all the requirements of claim 1, it is also important not to imply requirements which are not truly required by the claim. By way

of an example, the second indication must include a predetermined alarm associated with the detected predefined alarm condition, but that does not mean that the first indication cannot include a predetermined alarm. Equally, the fact that the first indication must include a temporary indicator (and must end before the second indication is output) does not mean that the second indication cannot include a temporary indicator.

Claim 5

172. I will mention Claim 5 very briefly, although Abbott submitted that, as the arguments have developed, claim 5 does not appear to play a role in the arguments. Claim 5 is for:

5	*The method of claim 1 wherein*
5.1	*the second indication is active at the end of the predetermined routine.*

173. Abbott submitted that this requires that the second indication (the "*alarm*" of integers 1.4, 1.5, 1.8) is output more or less straight away after completion of the *predetermined routine*. I agree that claim 5 seeks to specify a sense of immediacy of the second indication appearing at the end of the PDR.

INFRINGEMENT

174. Three Dexcom devices are contended to infringe EP627: the G6, G7 and D1. The infringement case was explained by reference to the G6 and its PPD and it appeared that no separate issues were raised by the other devices.

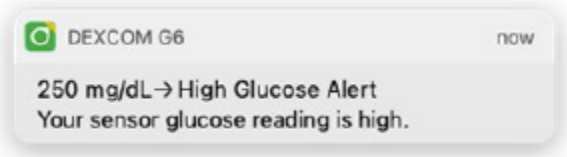
Abbott's case on infringement

175. As Abbott submitted, the G6 comprises a sensor and transmitter unit which attaches to the body to sense glucose levels, and a display device which receives information from the sensor/transmitter and displays it to the user. The display device can be an iPhone or an Android phone on which a dedicated app (the "G6 App") has been installed.

176. The example used by Dr Palerm in his Annex 2 to illustrate the infringement was as follows.

i) The infringement involves the G6 App running on the device in the background while the user is using another related app, such as the Dexcom Clarity App, to look at glucose reports. "[R]eview of historical data such as glucose data" is an example of a predetermined routine of integers 1.1 and 1.9 given at [0080].

ii) If the user is in the Dexcom Clarity App and, at that time, the G6 App detects an alert condition (integer 1.2), the phone will vibrate and/or sound temporarily (the "first indication" of integers 1.3 and 1.7), and at the same time generate an unobtrusive notification banner at the top of the screen to inform the user of the nature of the alert, which looks like this:



iii) Neither the temporary sound/vibration, nor the banner, generated by the G6 App, prevents the user from continuing with their predetermined routine (integer 1.6). In the words of EP627 [0078]: it "does not interrupt or otherwise disrupt the execution of the predetermined routine". There was reference in opening to a pleading issue based on the SOCI. This goes nowhere because satisfaction of the integer in question is now admitted, so the pleading has been overtaken by the admission and the evidence. The material above was in Dr Palerm's evidence served on 20 September 2022. Prof Oliver's evidence admitted that these features of integer 1.7 of the claim (the first indication and temporary indicator) is present.

iv) The banner generated by the G6 App may either be temporary (i.e. it disappears after several seconds) or persistent – the user is provided with the option in the settings for the G6 App. As a matter of common sense one would expect users to set it to persistent, given that it relates to a possible hyper- or hypoglycaemic alert. If the user selects the persistent option, it will stay unobtrusively on the top of the user's phone screen for as long as they continue to look at their glucose reports and without interrupting that routine.

v) The user can choose to finish their session on the glucose reports app by tapping on the banner; and at that point the G6 App will be brought to the foreground. So the "predetermined routine" will end, a pop-up window will be prominently displayed in the centre of the screen, and the rest of the screen will be greyed out, to alert the user to the condition that caused the banner to appear. The pop-up window with the greyed out screen is the "second indication", which satisfies integers 1.4, 1.5, 1.8 and claim 5, and looks like this:

vi) As can be seen, this is the standard, prominent alert that would come up if the user were not executing a predetermined routine. So in the infringement, like in the patent, the method provides for two separate kinds of indication. The first indication can be ignored by the user if they want; it does not interrupt or disrupt the task they are currently engaged in. The second indication is more prominent and requires acknowledgment.

Dexcom's non-infringement points

177. First, Dexcom says that the case relies on a separate app to the G6 App itself, but Abbott submitted it is not clear what the significance of this is said to be. They pointed out that there is no dispute that the data used by the Dexcom Clarity and Apple Health apps is that provided ultimately by the G6 sensor and the operations that they provide the user, including review of glucose data and trends, are routines associated with an analyte monitoring device. Moreover, the functionality that these apps provide complements that of the G6 App itself. Indeed, the Clarity app has been specifically designed by Dexcom "for uploading and viewing glucose data allowing them to view and generate a range of analyses and reports". As Dr Palerm explained, it is part of the G6 "ecosystem".

178. Second, Dexcom argue that the "*receiver unit*" of claim 1 is limited to the combination of the phone and G6 App, with the effect that involvement of any other app avoids infringement. Abbott submitted that is nonsensical on the basis that the presence of the apps turns the phone into an infringing device but the whole device is the thing that infringes. The phone receives the sensor data and the phone OS continues to perform the functions of a receiver unit, including providing notifications such as high and low glucose alerts, regardless of whether the app is in the foreground.

179. It seems to me that these first two points raise the same issue, essentially an issue as to the proper interpretation of 'receiver unit'. As I have held above, the addition of the Clarity App (or any other apps) does not convert what would otherwise constitute a 'receiver unit' into something which is no longer a 'receiver unit'.

180. Third, Dexcom emphasises that the claimed method may not be performed by every user on every occasion. But, as Abbott submitted, that is not an argument against infringement on those occasions when it is used. Nor does it change the fact that Dexcom programmed this functionality into its application. So there is nothing in these first three points.

181. Fourth, Dexcom says that the pop-up notification (i.e. the "second indication" in the scenario outlined above) does not function as a "reminder" since the user gets there by choosing to tap on the notification.

182. In closing, Dexcom sought to bolster this (and their other) non-infringement arguments with the contention that the infringement allegation made by Abbott does not achieve in the Dexcom devices the purpose or any of the advantages said to be given by EP627.

183. Dexcom contended that the first indication is not passive and the second indication serves no purpose. It does not act as a reminder. It does not provide any additional information. It simply requires the user to repeat the step of acknowledging the alert that was performed on the first indication and that triggered the second indication: in

the scenario set up by Abbott for its infringement case, the second indication is an annoyance – simply needing to be dismissed before the user can get on with doing what they want to do; simply telling the user exactly the same thing as the banner they have in the previous instant read, understood, and decided to click on. (Dexcom's emphasis).

184. Abbott argued that functioning as a "reminder" is not a requirement of the claims although it may be a feature of certain embodiments. The banner (together with the accompanying sound and/or vibration) is an indication which enables the user to continue. In contrast, the alert screen which comes up in the G6 App is a more prominent or permanent indication which requires acknowledgement from the user before they can do anything else in the G6 App. That combination of a first unobtrusive alert which does not disrupt the user followed by a second prominent notification that demands the user's attention is precisely the inventive concept of EP627.

185. A glance at the screen relied upon for the second indication shows Dexcom's argument in paragraph 183 above is factually incorrect. It is true both the banner and this screen provide the same low glucose alert (that, after all is a requirement of the claim that both indications are associated with the same predefined alarm condition), but tapping on OK on the second indication provides the user with access to the graph of his or her glucose levels over time, which may provide highly relevant information as to the rate at which the glucose level is falling.

186. In any event, as I have already held, there is no requirement that the second indication must be a 'reminder' in the sense inherent in Dexcom's argument. So there is nothing in this fourth argument.

187. Fifth, Dexcom referred in opening to the finding of non-infringement by the Mannheim Court on the basis that (it was argued) the second indication is not caused by completion of the predetermined routine.

188. Dexcom explained that their point arises from the contingent nature of the infringement allegation; in particular, that it relies on a very specific scenario in which the user has set things up in a particular way and is then interacting with the notification banner in a particular way and having a particular mental state (i.e. having decided they have 'had enough' of using Apple Health / Clarity and decided to exit by clicking on the banner, such that, when they click on the banner, it can be said that the predetermined routine has been 'completed' and not 'interrupted') when doing so, (integers 1.5, 1.6 and 1.7).

189. So, Dexcom submit that in the particular scenario relied on by Abbott the second indication does not come upon the completion of the routine. On the interaction with the first indication, the notification banner, the Clarity app is put in the background and the dedicated app brought to the foreground and with it the second notification. The second indication is thus neither *consequential* on the completion nor *sequential* to the completion but simply *co-incident* with it. It is the point that the Mannheim Court relied upon.

190. Abbott pointed out that this point was not put to Dr Palerm so it was not clear whether Dexcom still rely on it. In any event, Abbott submitted that, with the greatest of respect, the reasoning of the Mannheim Court was wrong, for two reasons. First, claim 1 merely requires the second indication to be output after completion of the predetermined routine. It is not limited to there being a causal relationship between the two. Second,

even if the claim was so limited, in the infringement case the second indication is caused by the user ending the routine by tapping the notification. So, the claim is satisfied in any event.

191. The argument is that the user taps or clicks on the banner at the top of the screen (the first indication), and thereby brings the PDR (which is the display of glucose data) to an end, whereupon the second indication appears.

192. In terms of processing, the alarm condition has been triggered and the second indication is 'waiting' to be output to the user interface. It is waiting on the completion of the PDR. So, the processor will be cycling through a short routine which periodically checks whether the PDR has completed. Once it has, then the second indication is output to the user interface.

193. In my view, in the infringement scenario, the output of the second indication to the user interface is caused by completion of the PDR. With respect to the finding of the Mannheim Court, I am not persuaded otherwise. I also disagree with the sleight of hand in Dexcom's argument (see paragraph 189 above). Whilst the dedicated app is brought to the foreground, I do not agree that the second indication is already sitting there and brought to the foreground with the dedicated app. Instead, the second indication is output on completion of the PDR. As is stated in the G6 PPD at [117(c)], 'To acknowledge this Glucose Alarm/Alert [i.e. the banner shown in 176 ii) above], the user may open the iOS G6 App, <u>whereupon</u> a pop-up window will appear [the pop-up window being that shown in 176 v) above]' (my emphasis).

194. I suspect that the real argument here concerned the interpretation of the PDR, with the argument being that a routine cannot be a 'a predetermined routine' if it can be brought to an end by the user. Any such argument would, in my view, be wrong. The execution of a routine may be brought to an end in a number of ways and I see no reason why what would otherwise be a PDR is not, simply because one of those ways was from input from a user on the user interface.

195. Having considered and rejected all of Dexcom's non-infringement arguments, and having considered Abbott's infringement analysis, I find the G6 infringes claim 1.

VALIDITY: NOVELTY & INVENTIVE STEP

196. Dexcom relied on three pieces of prior art, the **Dexcom STS Guide, Halpern** and **Bunte**. By the time of closings, Halpern had been dropped. So I need to consider whether the STS Guide anticipates claim 1 and obviousness over Bunte.

The STS Guide

197. The Dexcom STS Guide is the user guide to Dexcom's first CGM Device. Dexcom's anticipation case relies on a relatively small part of the Guide, which relates to the duration of the sensor session. Whilst the battery in the STS Transmitter lasts for up to 6 months, the sensor on the user's body is evidently considered safe for 3 days, after which the sensor is removed and a new sensor is inserted.

198. The STS Guide starts with overviews of the various components of the system, including the STS Sensor:

> The DexCom™ STS Sensor is a device that continuously measures your glucose levels. You will use a Blood Glucose (BG) meter to calibrate the readings measured by the STS Sensor. The glucose levels measured by the STS Sensor are sent by a wireless, low-powered, radio frequency (RF) to the STS Receiver every 5 minutes for up to 3 days (72-hours).

199. After the Sensor has been installed on the user's body and the various components are communicating correctly, there is a 2 hour start up period for the sensor to adapt to its new biological environment. Then the user must calibrate the sensor by reference to 2 finger prick blood glucose tests. Once successfully calibrated, blood glucose readings are taken from the Sensor every 5 mins for 72 hours.

200. Before the 72-hour sensor session period expires, the user receives the following notifications:

    i) A 6-hour STS Sensor Expiry Notification, on screen;

    ii) A 2-hour STS Sensor Expiry Notification, on screen;

    iii) A 30-minute STS Sensor Expiry Notification, on screen with an accompanying vibration;

    iv) A 0-hour STS Sensor Expiry Notification, on screen with an accompanying vibration.

201. The notifications on screen comprise an image of a hour glass which can be dismissed by the user pressing any button.

202. In the light of that disclosure, it is convenient to explain Dexcom's case by reference to the integers of claim 1:

Claim 1

1 A method, comprising:
1.1 executing, on a receiver unit (104, 106), a predetermined routine associated with an operation of an analyte monitoring device (1010);

203. The STS Guide is directed towards an analyte monitoring device. There are numerous routines disclosed but Dexcom focus on the measurement of the 3-day sensor session period. So the PDR is the routine which counts down to the expiry of the 3-day sensor session.

1.2 detecting a predefined alarm condition associated with the analyte monitoring device (1020);

204. The predefined alarm condition is the impending STS Sensor expiration. There is no question that this is one associated with the analyte monitoring device.

1.3 outputting, to a user interface of the receiver unit, a first indication associated with the detected predefined alarm condition during the execution of the predetermined routine (1030); and

205. The first indication is the 30-minute sensor expiry warning vibration.

1.4 outputting, to the user interface of the receiver unit, a second indication associated with the detected predefined alarm condition (1040);
1.5 wherein the second indication is output after the completion of the execution of the predetermined routine;

206. When the sensor session ends, a second indication is provided in the form of a 0 Hour notification.

1.6 the predetermined routine is executed without interruption during the outputting of the first indication;

207. The sensor session continues without interruption during the provision of the first indication.

1.7 the first indication includes a temporary indicator and,

208. The 30-minute warning vibration is temporary.

1.8 further, the second indication includes a predetermined alarm associated with the detected predefined alarm condition; and

209. On the basis that the predetermined alarm condition is the STS Sensor expiration both first and second indications relate to the same issue.

1.9 the predetermined routine includes one or more processes that interface with the user interface of the receiver unit.

210. It is self-evident that the PDR includes processes which interface with the user interface of the receiver unit. The user interface is both visual (on the screen) and tactile (the vibration) and amongst the relevant processes are the visual and tactile notifications.

Abbott's arguments against anticipation

211. I can deal with Abbott's arguments relatively succinctly, because, on analysis, they resolve to issues of interpretation of claim 1, which I have dealt with and rejected above.

212. First, Abbott submit that the 3-day sensor session period is not a PDR, as I understood matters, for two reasons: first, because it is not something which the user can choose to begin or end but its countdown to expiry continues regardless of the user's actions. They say this is nothing like reviewing historical glucose data or configuration of device settings. Abbott's second argument is to the effect that the 3-day sensor session period counter does not interface with the user interface: but it does, via the four alerts. These arguments carry no weight at all. As I have held, the expression 'predefined routine' is deliberately broad. I find the 3-day sensor session falls within the meaning of that term.

213. Second, Abbott argue that each of the alerts takes over the entire screen and requires acknowledgement by the user to clear the screen. I think this argument depends on Abbott's construction arguments that the first indication must be unobtrusive and the second more permanent. I have rejected both arguments. In any event, there is nothing in this second point.

214. Third, Abbott argue that each of the alerts relates to a different alarm condition – different times until expiry. This argument misunderstands the alarm condition on which Dexcom rely, which is sensor expiry. Abbott's further argument is that at each alert, the sensor is in a different condition. But this again confuses the status of the sensor with the predefined alarm condition, which is sensor expiry.

215. Accordingly, for the reasons explained by reference to Dexcom's case above, I find that EP627 lacks novelty over the STS Guide.

Bunte

216. In relation to Bunte, Abbott reminded me that while the skilled person is deemed to read the prior art with interest, they are not deemed to read it with any notion that it may be of any relevance or utility to their work, and that is particularly so when the prior art is located in a distant and unrelated field. See *Inhale v Quadrant* [2002] RPC 21, [47] (Laddie J):

> 'The notional skilled person is assumed to have read and understood the contents of the prior art. However that does not mean that all prior art will be considered equally interesting … A document directed at solving the particular problem at issue will be seized upon by the skilled addressee. Its very contents may suggest that it is a worthwhile starting point for further development. But the same may not be the case where a document comes, say, from a distant and unrelated field … The more distant a prior art document is from the field of technology covered by the patent, the greater the chance that an intelligent but uninventive person skilled in the art will fail to make the jump to the solution found by the patentee.'

217. Bunte is a patent application from 2006 entitled 'Method and Device for inhibiting interruption of a running application by an event'. Its abstract describes it as: "A methodology implementable in form of a hardware or software module for inhibiting interruption of a running application by an event according to a selected non-disturbance profile, said event occurring on a mobile device". It describes the operation of various "Do Not Disturb Modes" ('DDM') for use on, for example, a mobile phone.

Disclosure

218. Dexcom summarised the disclosure of Bunte in the following way. Prof Oliver drew attention to Bunte's identification of the state of the art it was addressing from line 26:

> 'According to the state of the art, a mobile device interrupts or pauses a running application if an incoming call for instance occurs. This is done by a pop-up message or similar and the user has to handle said pop up message for continuing using of said application. There is no possibility to set up a "do not disturb" behavior (or mode) within the running application which makes it possible to run said application without interruption.'

219. Bunte then goes on to explain that if, for example, you are gaming on your phone the only way to stop an incoming call interrupting your game is to switch off the telecom connection, which may not be possible if, for example, you need to connect to a game server while playing. Bunte aims to solve this sort of problem:

> "it is an object of the present invention to ensure proper continuation of running applications, especially games, even in case of incoming events."

220. Bunte's solution is to first detect an incoming event, check to see if a non-disturbance profile has been set and then interfere with the already running program according to the instructions given in the non-disturbance profile.

> 'In a first operation detecting of an occurrence of said event is provided. Afterwards, a determining if said non-disturbance profile has been set is provided. Then, inhibiting interruption of said running application according to said determined non-disturbance profile follows.'

221. Bunte doesn't just stop the incoming event taking over. It provides a "secondary indication" that doesn't interrupt the running program (Bunte uses 'intermitting' in the sense of pausing):

> "…said inhibiting is accompanied by a secondary indication without intermitting execution of said application if said non-disturbance profile is set. Thereby, a secondary indication to the user is provided, wherein said user realizes the occurrence of an event even if the application is not intermitted. The secondary indication may be in form of an audio notification for instance.

222. Bunte gives the example of an incoming MMS as the incoming event. It suggests that, in one scenario where CPU performance is at a premium, the MMS may not be fetched until after the running application is quit or paused:

> 'According to another embodiment of the present invention, said MMS is not fetched while said application is active and said non-disturbance profile is set. Because of the CPU performance increasing while fetching an MMS, it is preferred that said SMS is fetched later after quitting or pausing the foreground application.'

223. Prof Oliver compared the disclosure of Bunte to EP627. In his view, all the integers of EP627 claim 1 bar disclosure in relation to analyte monitoring devices is to be found in Bunte.

224. Dr Palerm read Bunte more restrictively. Although he accepted that the 'secondary indication' during DDM mode in Bunte was a first indication in the EP627 sense, he took the view that Bunte only disclosed two mutually exclusive options: either the secondary notification is provided to the user during DDM mode or the notification is suppressed entirely and a list of the supressed notifications is only provided to the user once the DDM mode has ended.

225. Dexcom submitted Dr Palerm was simply wrong on this point. Dexcom drew attention to the teaching in Bunte where the secondary indication concerns an MMS, but the message itself is not fetched until after the DDM mode has ended, to save impact on the GPRS bandwidth and the processing power of the device. I agree with Dexcom on

this issue. Dr Palerm was reading Bunte too restrictively. There is a potential further point that simply fetching the message and putting it on screen is not a second indication, but, even assuming that was what was contemplated in Bunte, it would have been entirely obvious to present a banner notification (possibly one of several) of the message which would then have to be selected to be opened.

226. On this basis, the big issue on Bunte resolves to whether the unimaginative Skilled Team would, having read and considered Bunte, think it had application to the environment they were considering – the operation of an analyte monitoring system.

227. I have considered the arguments from both sides carefully on this central issue. However, I have reached the clear conclusion that Bunte can only be seen as applicable with a good dose of hindsight. This is because there is one fundamental point of distinction between what is disclosed in Bunte and the method in claim 1 of EP627.

228. EP627 involves the inter-relationship between one aspect of an analyte monitoring device (the PDR) with another aspect of the analyte monitoring device (the 'alarm condition' of integer 1.2). Both aspects are 'associated with an/the analyte monitoring device'.

229. Bunte is concerned with suppressing notifications from one application (e.g. MMS/SMS messaging) in favour of a completely unrelated application (e.g. a game).

230. In this regard, it is notable that Bunte was introduced into the claim at a relatively late stage and well after Professor Oliver had seen and considered EP627.

231. I am inclined to conclude that Professor Oliver did not notice this distinction at all. In his first expert report, his reasoning was relatively brief:

> 'Although this predetermined routine in Bunte is not associated with the operation of an analyte monitoring device, I believe the Skilled Engineer would have no problem with applying the concept of Bunte to analyte monitoring devices. Indeed, it appears to me that the concept of Bunte is the same as that of EP 627 (as far as I have understood it): both involve notifying the user (in a temporary manner) of an event without interrupting a routine or while a program is running. When the routine or program has ended, the user is then notified of the event again (in a more permanent manner).'

232. Abbott had further points of distinction between Bunte and EP627, also related to that fundamental distinction. For example, they contended that Bunte would be implemented in the operating system software of the device and therefore its teaching was directed at a person responsible for producing operating system software for mobile devices. I think this submission confuses EP627 with the alleged infringement. EP627 is written around a dedicated analyte monitoring system, although it is capable of reading onto an analyte monitoring system operating on a mobile phone. I consider a person writing software for a dedicated analyte monitoring device would have to have the ability to write elements of the operating system. He or she would not set Bunte on one side as of no interest on this ground.

233. Dr Palerm was unshaken in his view that the skilled team in 2007 would have seen nothing of interest in Bunte. Abbott also submitted that ultimately Prof Oliver did not really maintain his view. At the end of his cross-examination, he was asked to consider Palerm 1 ¶15.16, which said:

> 'Furthermore, the DDM in Bunte is focused on the core functionality of a mobile phone, not interrupting a specific application. In that context, the DDM in Bunte suppresses incoming events from outside the application, such that the application in question (e.g., the gaming app) is not interrupted by those incoming events. As I mentioned in paragraph 7.42, at the priority date, the EP 627 Skilled Team would have contemplated that the receiver for a CGM would be a dedicated device only used to convey clinically important information to the patient about their glucose levels. It would, therefore, not be obvious to consider implementing the idea of Bunte in that context, namely in a dedicated receiver specifically designed to convey actual or potential safety critical information to the user. The same applies to claim 5.'

234. Prof Oliver was twice asked to consider that summary and identify whether there was anything that he disagreed with. As Abbott submitted, on neither occasion was he able to identify any points of substance.

235. The re-examination on the point was leading. Professor Oliver was specifically directed to the concluding statement and asked to consider "what he thought was unreasonable". He was only able to say that Bunte "can be read on to CGM in a very straightforward way", but that was nothing more than a reprise of his evidence in chief. He could not identify any reason why the skilled person would be motivated to adapt Bunte to fall within the claims nor any obvious route by which they might do so.

236. Therefore, in my view the Skilled Team of EP627 would simply set Bunte on one side as of no interest or application to their circumstances, particularly bearing in mind there is no specific defined problem facing that team. They are dealing with all the features of an analyte monitoring device, including records of readings and any alarms or alerts. The Skilled Team are not starting with any notion that an existing routine should not be interrupted by an alert or an alarm. Accordingly, they would read Bunte with interest to see what it disclosed but, in my judgment, they would conclude its teaching of not interrupting a game on a mobile phone, but giving a notification of e.g. an incoming message which would be fetched and displayed after the game play had finished, had no application to the operation of an analyte monitoring system.

237. Dexcom attempted to save the case of obviousness over Bunte by pointing to the fact that it not only taught external events (e.g. incoming calls or messages) but also mentioned internal events (a system alert, a clock alert, a low energy indication, a reminding task or the like). However, as Abbott pointed out, Professor Oliver did not rely on the teaching regarding internal events at all, and this seems to have been only picked up by the lawyers, possibly only after Dr Palerm mentioned the internal events in his second report. This focus on the teaching relating to internal events was itself the product of hindsight.

238. Accordingly, the allegation that EP627 was obvious over Bunte fails.

CONCLUSIONS ON EP627

239. For the reasons explained above, I find EP627 anticipated by the STS Guide, but not obvious over Bunte. If valid, the Dexcom devices would have infringed.

240. After I had completed the above section of this judgment, I was provided with a translation of the preliminary opinion of the German Federal Patent Court in relation to EP627, in advance of the oral hearing which has been set for 7 February 2024. The Court is of the preliminary view that EP227 lacks novelty over the STS Guide (D1) and lacks an inventive step over Bunte (D11) when combined with D1. It is pleasing to note that the Court has the preliminary view which coincides with my conclusion that the STS Guide anticipates. However, their consideration of Bunte is different to what I have had to consider, and their reasoning provides no reason for me to question my conclusion on Bunte.

EP223

241. EP223 is entitled 'Methods and articles of manufacture for hosting a safety critical application on an uncontrolled data processing device'. It claims a priority date of 08.09.2009, which was not challenged.

THE TECHNICAL CONTEXT OF EP223

242. Abbott were very keen to emphasise their contentions as to the technical context of EP223 at its priority date. Abbott contended as follows.

243. At the priority date of EP223, all CGMs on the market were dedicated medical devices comprising a sensor/transmitter and a dedicated reader/receiver bespoke to the device. The software running on these devices was bespoke to the manufacturer. It was subject to rigorous testing and regulatory approval prior to release to ensure that it operated correctly on the device.

244. This remained the case for several years after the priority date. It was not for another six years, in 2015, that the first mobile apps providing CGM functionality were released (Abbott's FreeStyle LibreLink app and Dexcom's G4 app).

245. Smartphone technology was also at an early stage of development. The first iPhone was released in 2007 and Apple's App Store, which first introduced the ability for users to download third party apps onto their phone, was launched just a year later in 2008, the year before the priority date of EP223. Although some mobile apps relating to health and wellbeing had started to appear by the EP223 priority date, these were effectively electronic diaries enabling a user to track by self-entry exercise, meals, sleep and so on. They did not provide a user with clinical data in real time on which actual treatment decisions would or could be made. They are a world away from medical devices intended to provide treatment for, or enable diagnosis and treatment of, potentially life-threatening conditions.

246. These contentions underpinned Abbott's case on the composition of the Skilled Team, their CGK and the level of their interest in developing apps to run on smartphones. In this regard, Dexcom submitted that Dr Palerm's written evidence contained only the scantest acknowledgment that the implementation of safety-critical medical device functionality in smartphone apps was something of interest to the Skilled Addressee in September 2009. What he said was:

> '… As smartphones gained popularity, the teams designing CGMs, or insulin pump systems, started thinking about how to make this happen. Although <u>by 2009 this may have been contemplated as a theoretical possibility</u>, the EP 223 Skilled Team would have known that doing so had the potential for serious consequences to the user if it turned out that other applications or a new operating system release could lead the medical application to fail or operate improperly. …'

247. I agree that Dr Palerm's written evidence greatly understated the interest which real skilled teams would have had in transferring safety-critical functionality into smartphone apps. This was accompanied by an apparently conscious downplaying of

the state of smartphone technology in September 2009: Dr Palerm asserted that "*smartphone technology was in its infancy"* and that the functionality and apps of the first iPhone (which did not have an app store) was "*minimal"* – but failed to mention anywhere in his evidence the iPhone 3G and 3GS (which were more advanced, had access to an App Store with more than 50,000 apps and had sold millions of units in a matter of days). In cross-examination, Dr Palerm agreed that the functionality of the apps available to the iPhone 3GS was not "minimal" in 2009.

248. It became quickly apparent from Dr Palerm's cross-examination that regardless of whether the technology could have been said to be in its "infancy", he agreed that the idea of hosting safety critical applications (SCAs) – and specifically CGM readers – on smartphone devices was widely viewed as attractive in September 2009. I refer to the following passages in his cross-examination:

> 'Q. You do not suggest that people working on a CGM device before the priority date would not have thought of the idea of transferring the functionality of a dedicated CGM reader or an insulin pump controller into a smartphone app, do you?
>
> A. No, not at all. In my context, working in this industry, we were thinking about it. The question was, "How? How do we keep the same level of control and certainty that the application is going to run predictably and reliably as in our self-contained ecosystem where we control everything?" … So the questions were really about not that we would not want to do, it but how would we be able to achieve it and be comfortable that it is going to continue to perform as expected.
>
> …
>
> Q. It takes up room in your pockets or bag; yes? The more things you have, the more you have to lose and so on. It is very frustrating if you leave them behind. So if you can cut down the number of different bits of equipment that a person with diabetes has to carry around with them, that is obviously a very desirable thing; yes?
>
> A. Oh absolutely. In every single diabetes medical device company that I have worked at, we have an (indistinct) presentation [overrepresentation?] of people with type 1 diabetes. They want to work in the industry, because they have the disease and they want to be part of the solution of coming up with better devices that will help them and other people like them. So yes, it is definitely in their minds.
>
> ….
>
> Q. Here , you are making the point that I think you have just made about the safety concerns, but you say in the middle of that paragraph, "although by 2009 this", and by "this" you mean putting the software on a smartphone, "may have been contemplated as a theoretical possibility", I think would it be fair to say it was a bit

> more than that? People were actively excited about it and would like to do it. You say they had concerns, but they were thinking about it actively; yes?
>
> A. Yes.
>
> ….
>
> Q. What this article demonstrates very clearly is that people were looking ahead in 2009 to a future in which diabetes equipment was integrated into the smartphone, yes?
>
> A. Yes.
>
> ….
>
> A. No. At this point in time, I am working on Medtronic diabetes. We are having these conversations precisely around how to port CGM into a mobile phone.
>
> Q. You were actively engaged at the time?
>
> A. Yes.
>
> Q. Not as a theoretical possibility, but something you were really trying to do?
>
> A. There were conversations of how could we make this happen? There were people at the company that went out and met with people at Apple and that is how I know that the answer from Apple was, "No, we will not share a pre-released version of our new operating them with you. You will get it at the same time as everybody else will get it". Those type of questions are the main obstacle of how do we work around that?'

249. In this regard, as I indicate below, both Dr Palerm and Abbott significantly downplayed the level of interest and knowledge of the Skilled Team in writing apps for smartphones by the Priority Date of EP223. The fact that it took six more years for the first mobile apps providing CGM functionality to appear on the market is an indication of the long development times required to develop not just the software but also the complete CGM system. However, by the Priority Date of EP223, it is clear that the idea of putting the functionality which resided on the dedicated devices on the market into an app running on a smartphone was both obvious and well known in the field. That is not to say that there were not challenges which the Skilled Team had to overcome.

THE SKILLED TEAM OF EP223

Composition of the skilled team

250. The arguments over the composition of the skilled team were reflected in the disputes over CGK. The experts agree that the skilled person/team in relation to EP223 would

be – or include – a software engineer or software architect. However, there was some disagreement between the experts as to the software engineer's experience and field of activity. Dr Palerm's view is that the software engineer's background would be in designing software for dedicated medical devices, CGMs in particular. In contrast Dr Stirbu assumed that the software engineer would be someone who worked on "*health-related software applications including for mobile devices*". He considered that Dr Palerm's focus on medical devices and CGMs in particular was overly narrow.

251. Abbott criticised Dr Stirbu for apparently ignoring the fact that the claims are specifically directed to a method for use with an analyte monitoring device and/or drug administration device, and that the paradigm examples of such devices described in EP223 are heavily regulated medical devices – CGMs and insulin delivery devices (see [0003]).

252. Abbott submitted that it was well established that the skilled person is the skilled person or team within the established field – which may be a field of research or of manufacture – within which the problem addressed by the patent is located (see the recent summary of Meade J in *Optis v Apple (Trial C)* [2021] EWHC 3121 (Pat) at [29] – [31]). The design of such devices was an established field of manufacture, and it is that field to which the patent is directed in this case. The skilled person/team is therefore a software engineer working on the design of analyte monitoring devices/insulin delivery devices, and their background and experience would be in the design of software for such devices. Abbott submitted that Dr Stirbu's definition of a person working in "*health related software devices including for mobile devices*" was too broad.

253. Abbott acknowledged that this distinction did not appear to have given rise to any significant difference in the skilled person's core skill set. The significance of the distinction, according to Abbott, lay in the skilled person's understanding of the specific requirements of developing software for controlling analyte monitoring or drug administration devices. Conversely, Abbott submitted that the way in which Dr Stirbu understood the skilled person wrongly built in an assumption that their focus is on designing software applications for mobile phones or other UDPDs rather than methods for use for analyte monitoring devices. Thus, Abbott's point was that Dr Stirbu's definition of the skilled person built in an aspect of hindsight.

254. Dexcom's response to all of Abbott's points was straightforward. In essence, Dexcom submitted that Abbott had mixed together three separate issues:

i) First, the technical capabilities of the Skilled Person/Team. Perhaps not surprisingly, there was no dispute that they would be able to write the software to implement the teaching of EP223.

ii) Second, what was happening in the field. Dexcom submitted that Abbott were incorrect in saying the only experience of the Skilled Person/Team was in writing software for dedicated medical devices. Dr Palerm's own experience at the Priority Date (when he was working for Medtronic) was that people at his company were in discussions with Apple over whether they would be able to obtain a pre-release version of the latest iOS. There was nothing to indicate his experience was unusual. In other words, persons in the field were actively working on the idea of moving functionality previously held on dedicated devices onto smartphones.

iii) The consequence of that second point was that, even if a software engineer working on the design of analyte monitoring devices only had experience of writing software for dedicated devices, he or she would either have to acquire the appropriate knowledge of writing software for smartphones/UDPDs or the team would be supplemented by someone with that knowledge (e.g. by bringing someone in with the type of experience of Dr Stirbu).

iv) Third, the degree of interest which the Skilled Person/Team would have had in utilising a smartphone to provide the functionality previously contained in the dedicated devices – this is effectively Abbott's hindsight point.

255. It is clear, in my view, that Dr Palerm and Abbott sought to play down, to a significant extent, the interest which those in this field had in utilising smartphones to replace the dedicated devices in the market. In my judgment, EP223 was clearly addressed to a person or team which straddled both the pre-existing dedicated devices which required the writing of bespoke software and the more recent requirements of writing software for use in the smartphone environments which were, by the Priority Date, already well established and clearly predicted only to grow in significance. Although Abbott limited the claims by amendment such that the UDPD is a mobile phone, EP223 was also addressed to other UDPDs, not just dedicated devices but also tablets, laptops and PCs. This last point has consequences for the scope of the CGK.

CGK for EP223

256. With the dispute over the composition of the Skilled Team resolved, the resolution of many of the disputes over the CGK is straightforward. What follows in this section is largely agreed, but I have also resolved some of the minor disagreements.

Mobile phones / health applications

257. The statements made in this section constitute part of the CGK of the skilled addressee of EP223 at the 2009 Priority Date.

CGM devices

258. In September 2009, the available CGM devices were supplied with dedicated readers/receivers upon which the bespoke manufacturer's software was loaded. In this way, CGM and other medical device manufacturers ensured that the software used by patients for making critical decisions about their treatment or health was carefully controlled and tested prior to release.

Mobile phones

259. As of September 2009, there were different kinds of devices on which mobile and web-based applications could be installed and used, one of which was the smartphone, which is a mobile phone which has computing and mobile communication functions in the same device.

260. The skilled addressee of EP223 would have been familiar with the general features and limitations of a smartphone at the time.

261. In terms of hardware and appearance, in the mid-2000s, a lot of the smartphones had a physical keyboard (like the Blackberry devices shown below), but from around 2007 there was a major shift away from physical keyboards to ones with large finger-operated touchscreens (like the LG and Samsung devices shown below).

Blackberry Pearl (2006)

BlackBerry Curve 8330 (2007)

BlackBerry Bold 9000 (2008)

LG Prada KE850 (2007)

Samsung F480 Tocco (2008)

262. Apple's iPhone was first introduced in early 2007 (shown below). It had a relatively large capacitive touchscreen (for that time), introduced multi-touch interaction to phones and in terms of the software its OS (iPhone OS, "**iOS**" 1.0) was capable of running Apple's web-browser that could easily open full websites which were not specifically designed for phones.

iPhone 1 (2007)

263. By 2008, Apple had released the iPhone 3G. This came with an updated version of iOS, the iOS2. With the iPhone 3G and iOS2 came Apple's 'App Store', which was built in on the device and allowed the user to download third-party software onto the iPhone.

Apple iPhone 3G (2008)

264. By the 2009 Priority Date, the following mobile platforms (operating systems) were available:

Platforms	Version	Programing language	Device lead
Android	1.5	Java	HTC
iPhone OS	3	ObjectiveC	Apple
PalmOS	1	JavaScript	Palm
Windows Mobile	6.5		Compaq/Microsoft
S60	5th edition	Symbian C/JavaME	Nokia

265. The skilled addressee of EP223 would be aware of, or be able to obtain information on, the features and capabilities of the following mobile phones that were available before 8 September 2009. Accordingly, they would have known that each of the mobile phones below included the capability to download and install third party applications

and would have been aware of the operation and features of the Apple App Store, Android Marketplace, Palm App Catalogue, Windows Marketplace and Ovi Store.

iPhone 3G;

HTC Hero;

Palm Pre;

Samsung Omnia i900;

Nokia N97.

266. There was no disagreement that the skilled person would have a general knowledge of the mobile phones that were available at the 2009 Priority Date, their general features and limitations, and some familiarity with their operating systems.

Installation checks

267. By 2009, both the iOS (Apple) and Android (Google) were using digital signatures to verify the integrity of app installation packages and to confirm that the app had installed correctly on the mobile device.

Regulatory considerations for medical device software

268. Medical products are heavily regulated at several levels:

i) Regulatory frameworks: e.g., US (HIPAA, FDA) or EU (Medical Device Directive) legislation;

ii) Local legislation and rules: e.g., US state or EU member state level;

iii) Guidance documents: FDA or Medical Device Coordination Group ("MDCG");

iv) International standards: ISO and IEC standards e.g., ISO 13485 (Medical devices – Quality management systems – Requirements for regulatory purposes), ISO 14791 (Medical devices – Application of risk management to medical devices) and IEC 62304 (Medical device software – Software life cycle processes), IEC 62366 (Medical devices – Application of usability engineering to medical devices).

269. Medical software needs to be developed according to well defined practices that ensure that the device is safe and effective. Medical devices may also need to be validated through clinical trials. If the product is also operated by the manufacturer as part of a service, they need to ensure that the operations are compatible with the appropriate legislation (e.g., HIPAA in the US).

270. In order to ensure this, the device manufacturer needs to establish a quality management system compatible with IEC/ISO 13485 and perform risk analysis according to ISO 14971. Additionally, the manufacturer needs to establish working processes compatible with IEC/ISO 62304 that govern software development lifecycle.

271. The skilled addressee of EP223 would be directly familiar with the content of the standards or regulatory requirements relevant to medical devices, or would work closely with regulatory, risk management and clinical trials specialists who would have this knowledge.

The Disputes on CGK

272. Dexcom identified the following points on CGK which were in dispute:

i) Knowledge of the advantages of the iPhone and Android platforms

ii) Knowledge of the multitasking platforms and their limitations

iii) The sophistication level of smartphone technology and applications in 2009

iv) Knowledge of healthcare related mobile apps and relevance to safety critical software design

v) CGM devices were supplied with dedicated readers

vi) Regulatory expectations for medical software validation

vii) Knowledge of specific software verification techniques and relevance to safety critical software design

viii) Knowledge of general approaches to medical software development and verification.

273. Each of these issues stemmed from the differing views which Drs Stirbu and Palerm took as to the composition of the Skilled Team and their experience. In view of my conclusions on the context and the composition of the Skilled Team for EP223, I can resolve the remaining disputes on their CGK relatively succinctly.

274. Although Abbott disputed Dr Stirbu's view that a range of health and wellness applications were available on mobile platforms in 2009 and would have been CGK, I find Dr Stirbu's views properly represent the CGK. Dr Stirbu also said that the skilled person would have appreciated the potential for mobile phones to be connected with medical devices.

275. In general, I accept Dr Stirbu's evidence on each of these issues. What follows is my edit of certain paragraphs taken from Dr Stirbu's reports. All of the following was CGK.

276. Apple's iPhone, the App Store and its SDK were considered revolutionary when they were released in 2008, the App Store and the SDK became the new exemplary standard for smartphone platforms, particularly in relation to software development, distribution, installation, security and payment. One of the most significant aspects of the iPhone SDK was that it provided a holistic developer experience with tight integration of the development environment (called XCode), a device simulator, and integration with the Apple's AppStore servers. Installation and use of the development environment was as simple as for any Mac application. In contrast things were more complicated on some other platforms at the time. For example, in Dr Stirbu's experience, configuration of

the development environment for Nokia's Symbian/S60 platform (discussed further below) could take about one day following the instructions provided.

277. Android (developed by Google) also had potential at the time, although it was not as widely adopted as iOS due to the limited availability of Android devices at the time.

278. Another area in which mobile platforms in 2009 were limited was support for multitasking. Multitasking refers to the ability of a platform (operating system and hardware) to run several applications simultaneously. This requires the system to allocate resources (e.g. processor time, memory and access to peripherals) between several applications simultaneously. In a true multitasking operating system, either several applications could be displayed on screen at once, or one application could be on-screen (in the foreground) while other applications continued to run (e.g. perform calculations, receive inputs/provide outputs) in the background. This was a feature of all common PC operating systems in 2009, but was not generally available in mobile devices.

279. iOS tried to give users the impression of multitasking, by taking a snapshot of an application when it was moved to the background. The app would be restored (i.e. restarted) from that snapshot when the user brought it back to the foreground (e.g. by selecting it in the app switcher view). This gave the impression of multitasking, but in reality, each third party application was terminated when it was moved to the background.

280. Android, as a Linux derivative, had the ability to run multiple applications at the same time although the contemporary devices' hardware limitations would restrict the use of this capability. Although apps could in principle run in the background on an Android system, in practice they were liable to be forcibly closed by the operating system in order to save hardware resources.

281. Nokia also had its own mobile OS at the time, called Symbian, which was different from others in that it was advertising its ability to run multiple applications simultaneously. However, in practice Symbian was very difficult to develop applications for and was not widely used. Although the skilled person would have been generally aware of Symbian and its capabilities, a detailed knowledge of how to develop Symbian applications would not have been part of the CGK.

282. Health and wellness applications were also available for various mobile platforms in 2009. As for medical applications, smartphones were becoming more and more widespread in around 2009, and they came with various connectivity functions, like Bluetooth, which enabled them to be connected to other devices. As such the potential for medical applications for mobile phones and for mobile phones to be wirelessly connected with medical devices would have been appreciated by the skilled person at the time. Dr Stirbu recalled terms like "mHealth" being used at the time.

283. Despite the leaps made by Apple and others, developing mobile applications in 2009 was not necessarily a quick or easy process.

284. Troubleshooting was common in 2009 for numerous reasons. For instance, a company developing an app generally needed to have the physical device the app was being developed for, as often the mobile device emulators (or simulators) available at the time

were not an exact match of the real hardware. As an example, an emulator running on a PC would not have access to certain hardware capabilities of the mobile device, such as Bluetooth. These features would have to be tested once the software was installed on the real hardware. Distributing apps to testers and collecting feedback from the field (e.g. the app running on user's devices) during beta or final releases was not easy. Large companies would have had their own testing departments or hired specialised test companies to test and collect the feedback. However, for smaller companies or even individual developers this would have been impossible. TestFlight fixed this in 2010 by providing a system that simplified tester enrolment and viewing feedback via an online dashboard. Prior to this development, teams would have to develop their own solutions which added to the complexity. The skilled person would have appreciated these kinds of issues.

285. Developers of web-based applications had access to a larger body of information. Simple object access protocol ("SOAP") based applications have been developed for years and the representational state transfer ("REST") APIs were gaining traction. Both approaches were well documented in literature and good commercial and open-source implementations (e.g. Java, Python) were easily available, and therefore this would have formed the CGK of the skilled person.

286. Dr Stirbu was asked to comment on how, in 2009, the skilled person would ensure that a software application installs and operates correctly, both during the development process and when in use by the end user. He gave the following explanation.

287. For mobile applications, various techniques to verify the integrity and authenticity of apps were already known and being used in 2009. The most common examples at the time (and still are to this day) were digital signatures and certificates, which were routinely used, including by Apple and Google, to verify the integrity and authenticity of applications. Specifically, both the iOS (Apple) and Android (Google) were using digital signatures to verify the integrity of app installation packages and to confirm that the app had installed correctly on the mobile device – this feature was included in iOS since the release of iOS 2.0 in 2008 and in Android since its initial release in 2008.

288. The digital signature and certificate process used by both iOS (and Android) at the time worked as follows (and it continues to work in the same way to this day):

i) The developer compiles the application as an installation package for the App Store (or Android Marketplace).

ii) This installation package is digitally signed by the developer and then sent to Apple, i.e. uploaded to the App Store (or Android Marketplace).

iii) Apple (or Google) verifies the installation package conforms to the rules of the platform (e.g. appropriate content, use of approved APIs, no malware bundled in the app, no deceptive behaviour) and adds its digital signature. The application then becomes available for download/purchase on the App Store (or Android Marketplace).

iv) At a high level, when a user downloads the app (e.g. by selecting "Buy Now" or "Install" button on App Store – later changed to "Get"), the App Store app (or Android Marketplace app) on the user's phone and its operating system, iOS

(or Android), check (i) the digital signature of Apple (or Google) to verify that the file has been certified by Apple (or Google), (ii) the digital signature of the developer to verify the identity of the developer and (iii) the integrity of the installation package.

289. In essence, the digital signatures (from the developer and from Apple or Google) confirm that (i) the app has been verified by Apple (or Google), (ii) the app was created by a known sender (the developer), and (iii) that the files in the installation package have not been modified/altered in transit, before beginning installation. In effect, the digital signatures are a promise by Apple (or Google) that "yes, this person (the developer) is who they say they are, and we, Apple (or Google), certify that".

290. In iOS, a similar digital signature check is performed each time a user launches an app. The same digital signatures described above are used to verify that the installed app files are correct and have not been modified, prior to launching the app.

291. The skilled person would have been familiar with the digital signature process used by iOS and Android in 2009, as described above. It is one of the reasons that allowed iOS (and later Android) and smartphones to become widespread, popular, and easy to use (from the user's perspective). It is relatively simple yet effective, which is why the general principle has not changed since then and the process continues to be used in the same way on the modern-day versions of the iOS (App Store) and Android (Google Play).

292. Outside of the mobile phone context (e.g. in relation PCs), digital signatures had been in widespread commercial use since at least the 1990s. Similar principles to those discussed above were used to verify software with these types of digital signature. As such, the skilled person would be familiar with the general principles and application of digital signatures to verify software installation.

293. The checking of the integrity of the files referred to in (iii) above is a more sophisticated version of basic verification processes such as Cyclic Redundancy Checks ("CRCs") and hash functions. CRC functions have been widely used for error detection since the 1960s. A CRC is a mathematical function in which a unique value is calculated based on the data in a file. This number, known as a checksum is then attached to the file. After the file is copied or transmitted, the checksum is re-calculated and compared to the checksum attached to the file. If the two checksum values differ, there is an error in the file.

294. CRCs are part of the broader group of 'hash functions' which are used to calculate a unique number (a hash value) of a fixed length (e.g. 32 bits) from a larger block of data, although the output length of a CRC is much shorter than the type of hash functions used in cryptography (e.g. 16-64 bits vs 96-512 bits). The process of calculating a hash value is one-way, in that the original data cannot be recreated from the hash value. Hash functions form the basis of many verification processes including digital signatures and certificates. CRCs are generally used to verify that files have not been corrupted by transmission/storage medium errors, while the cryptographic hash functions are used to prevent interference from active attackers in the landscape.

295. In addition to the signature checks described above, typically, the OS ensures that the applications are initially installed in secure sandboxes where third parties do not have

access. 'Sandboxing' is a technique for separating programs by typically providing a highly controlled environment in which to execute an untested or untrusted program or a program which is being executed for the first time by the OS. This ensures that one application cannot modify the files of another application, possibly preventing the application from functioning correctly. As such it is frequently used to test programs that may contain a virus or malicious code without the risk of the software harming the host device/OS. The principle of sandboxing has been well known in the software development and IT security field since the 1990s. This approach has been a well-known feature of iOS since its initial release in 2007 and has also been available in Linux (an operating system for personal computers) since at least 2000. As such, the skilled person would be well aware of these methods for ensuring an application is able to install and operate correctly.

296. Other techniques used in cybersecurity can also be integrated in the application, in addition to the capabilities provided by the OS. For example, on Android devices data created after installation that can be stored on memory cards can be secured using techniques like cryptographic hashing to ensure that it has not been changed by unauthorized parties.

297. Other general strategies used to detect and mitigate errors in software applications in 2009 (and now) included: (a) Installing software on multiple devices (e.g. the Android ecosystem consisted of multiple devices produced by different manufacturers, with differences in processor speeds, memory size (RAM or storage), screen size, and components that communicated with peripherals. These devices could behave slightly differently, so testing on actual hardware was needed); (b) If the application becomes corrupted after installation, the OS would have some capacity to monitor and mitigate any errors. For example, Symbian Platform Security, introduced in Symbian OS v9 (around 2006) provided a secure folder for each application installed on the internal memory. The secure folder was protected from other applications. For the apps installed on removable media, the operating system stored a reference hash in a tamper proof internal memory area and computed and compared the hash whenever the application was run. Overall, this mechanism is equivalent to the process used on iOS, discussed above.

298. The techniques described above to ensure applications installed correctly were also well known in PC systems prior to 2009. For example, Debian Linux had a distribution system for third party applications which mirrors the process described above. An application developer prepares an installation package, which is an archive comprising the application data and a control file. The control file includes details of the supported hardware and possible conflicts with other software packages as well as cryptographic signatures to verify the contents of the installation package. This installation package is submitted to a central repository (the Debian server), where users can subsequently download the application. The Debian OS checks the installation package and installs the application. Where the installation fails, an error is displayed, although it is possible for a user to override the error and launch the application anyway.

299. In addition to the methods described above to ensure applications installed correctly, there were a range of checks used to ensure software would run as intended. For example, Microsoft introduced the Windows Experience Index ("WEI") in Windows Vista in 2007. WEI checked the hardware capabilities of a user's PC and provided a score indicating how well Windows would run and which features should be enabled

for best performance. There were also lots of applications (e.g. video/audio, media or gaming applications) that checked the length of time certain actions took to determine if the application could be run properly on the device depending on whether or not there was too much delay because the hardware was insufficiently powerful. Similarly, display checks were commonly used to ensure software for any kind of display device operated properly. An example of this is professional graphics applications where you need to calibrate the screen to get the proper tones, and ensure images are displayed correctly (e.g.to accurately match printing).

300. It was also common to check the hardware and software environment on a PC to determine (a) if the system met the minimum requirements to run an application (e.g. WEI discussed above) and (b) if the system had changed since installation in a way which might affect the performance of the application. An example of this process is the Microsoft Windows Genuine Advantage ("WGA") program. WGA was an antipiracy program which applied to Microsoft Windows from July 2005. WGA validated the installed copy of Windows and its licence key to determine if it was licensed by Microsoft. The installed copy of Windows was then matched to the hardware configuration of device it was installed on. If WGA determined that the copy of Windows was not genuine (i.e. not licensed by Microsoft), or there had been a significant hardware change, a message would be displayed to the user and access to non-critical Windows update functionality was disabled.

301. In 2009, a range of techniques were available to developers to ensure software installed and operated correctly, depending on the type of medical device involved. All of the verification techniques described in paragraphs 286-300 above would equally apply to medical software being installed on mobile devices. In addition, as medical devices are purpose based, it is possible to clearly define the boundaries of how the application is intended to be used, which makes the testing process simpler. The general process for developing a medical software application is outlined below and includes the following steps:

(a) Identifying user needs;

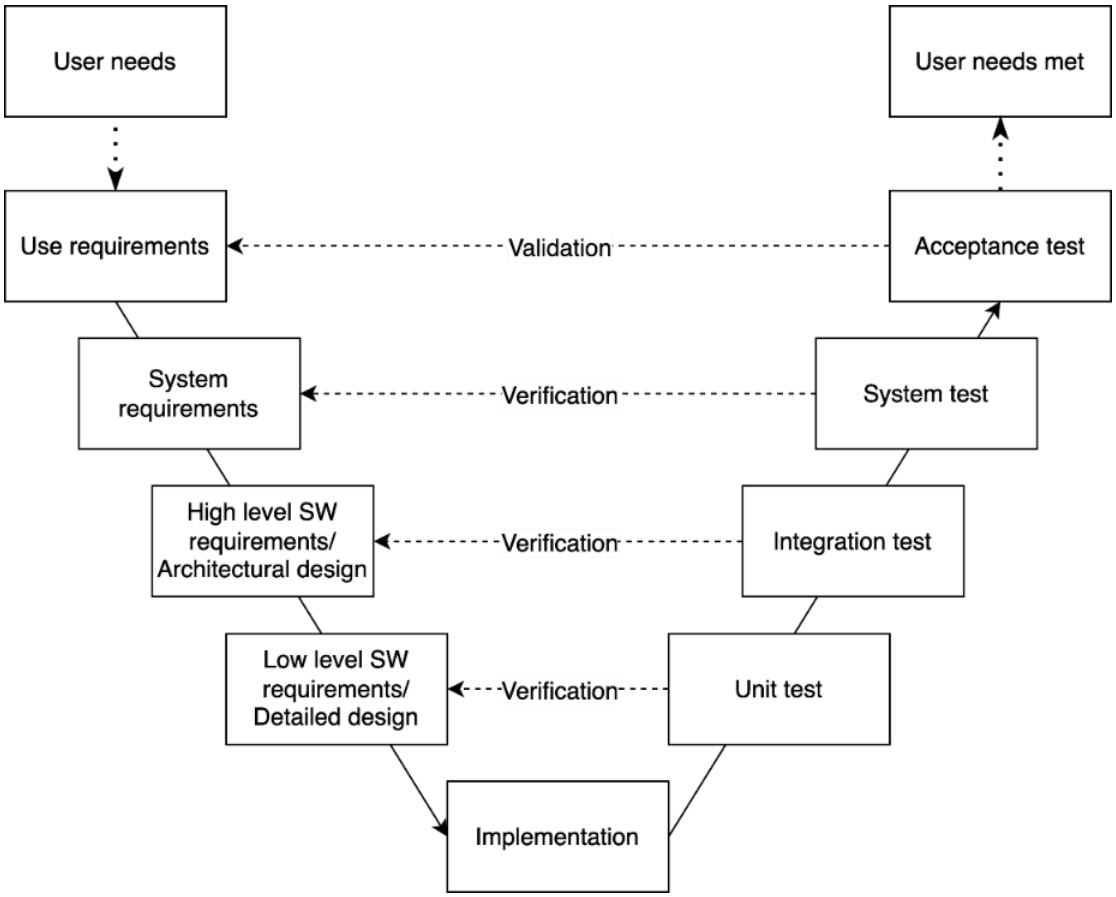
(b) Converting user needs into system requirements, which establish the purpose of the device and serve as inputs for the software design process;

(c) Transforming system requirements into high-level software requirements which set out the architectural design of the software;

(d) Further refining the high-level software requirements to give low-level requirements and a detailed software design, which serves as the design input for implementation;

(e) Developing the software application based on the detailed design. The resulting software code, test cases and documentation serve as design outputs; and

(f) Validating the product against the intended use. This is performed at unit test, integration test, system test and acceptance test level.



302. The approach above, derived from the V-Model introduced in 1991, is a well established method for designing regulated products, such as medical devices, which ensures effective risk mitigation and compliance with regulatory requirements. This has been included in regulatory guidelines since at least 1997 and would have been familiar to the skilled person.

DISCLOSURE OF THE PATENT

303. In summary, EP223 relates to methods for ensuring that "*Safety Critical Applications*" ('**SCAs**'), can be installed and operate as intended on an "*Uncontrolled Data Processing Device*" ('**UDPD**'). A UDPD is a device, such as a mobile phone, on which the user is permitted to make changes to software or hardware ([0005]).

304. EP223 is concerned with "safety critical" software applications. The Patent starts in [0001] with essentially a definition of safety critical systems. These are systems whose "failures or malfunctions may result in significantly detrimental consequences such as death or injury to persons, severe damage or loss to equipment or to environment". Medical systems are identified in [0003] as an example of "*safety critical systems*", including analyte monitoring devices, including glucose meters.

305. EP223 then focuses on safety critical applications ("**SCAs**") and seeks to address problems which may arise when a SCA is installed on an "*uncontrolled data processing devices*" ("**UDPD**"). UDPDs are data processing devices which "*permit the user to make hardware and/or software changes to the device – e.g., installing/removing software programs, installing/removing drivers, adding/removing hardware components, etc.*" (see [0005]). Examples of UDPDs include "*personal computers (e.g. desktop, notebook, etc.), mobile phones (e.g., iPhones®, Blackberry®, etc.), personal digital assistances (PDAs), etc.*"

306. A UDPD is contrasted with a "controlled" safety critical system: "Once the entire safety critical system have [sic] been verified and validated, the entire system is released and is not expected to undergo software and/or hardware changes. This provides for a very controlled system environment. New software and/or hardware changes are not introduced into the market unless and until the new hardware and/or software have undergone a new validation process. Such a controlled system environment provides a certain level of confidence that the system will not be altered or changed and potentially affects the proper operation of the system" (see [0004]).

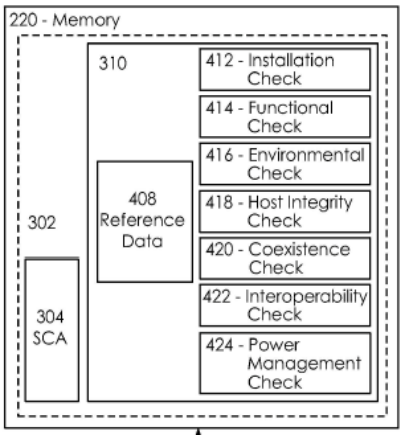
307. The crux of the problem which EP223 seeks to address is that "…the uncontrolled nature of the data processing devices compromises any assurance that the SCA will operate, or continue to operate, properly on the UDPD" (see [0005]). The way EP223 seeks to address this problem is by providing that: "[v]arious combinations of checks (e.g., installation check, functional check, host integrity check, coexistence check, environment check, etc) are executed at various times to determine if the SCA may operate properly on the device. The operation of the SCA on the UDPD may be controlled accordingly" (see [0006]).

308. EP223 provides a more detailed explanation of the kind of problems which may be encountered when an SCA is installed on a UDPD at [0022]:

> 'When a SCA is installed on a UDPD, there are no assurances that the SCA will operate properly on the UDPD because there has been no verification or validation process performed after the SCA is installed on the UDPD. The environment of the UDPD is dynamic and can change in a way that effects the proper operation of the SCA on the UDPD. For example, various software programs and drivers may be installed and removed from the UDPD and not only change the processing environment of the UDPD, but also may consume processing bandwidth making the UDPD process other applications more slowly. Various software configurations may be changed as well, which may affect the processing environment of the UDPD. Furthermore, changes to hardware components (e.g., wireless cards/modems, etc.), or configurations thereof, may affect the proper operation of the SCA on the UDPD (e.g., prevent communication to an external device). Still further, activities of the user may lead to the system obtaining viruses or spyware that can change the environment of the UDPD or consume processing bandwidth and prevent the SCA from operating properly. Moreover, changes to the system may impact power consumption of the system which may compromise the SCA.

> Thus, the uncontrolled nature of the data processing devices compromises any assurance that the SCA will operate or continue to operate properly on the UDPD.'

309. The solution provided in EP223 is a method of performing tests or checks with a UDPD, to ensure the SCA continues to operate properly. These checks may be incorporated into a test module referred to as a "*test harness*", although this appears to be a preferred embodiment and the claims do not require a test harness. The test harness and SCA may both be installed on the UDPD as part of the same program module, or they may be separate programs which are validated and installed separately ([0053] – [0054]) or the test harness may be included in the SCA [0055]. Thus, the "test harness" is distinct software responsible for performing the "*various combinations of checks"* with which EP223 is concerned. This is illustrated in the following part of Figure 4 (described at [0056] – [0063]):



310. This is a block diagram showing the way in which software is stored in the memory (220) of the UDPD. Note:

i) the SCA itself is the relatively small block 304;

ii) the "test harness" is the larger block 310;

iii) the SCA and test harness may be parts of a larger program 302;

iv) the test harness comprises:

a) stored reference data 408; and

b) seven different kinds of checks each depicted in its own box 412 – 424.

311. The description of EP223 is focussed on the seven kinds of check depicted as components of the test harness in Figure 4, of which those of principal relevance to the claimed subject matter are "*an installation check*", a "*functional check*" and an "*environment check*". Each kind of check is clearly envisaged as being different from the others and each is presented as having its own particular purpose.

312. Before discussing the individual checks, it is helpful to understand some general teaching in the specification (which comes before the detailed explanation of the

individual checks). First, as to the way in which EP223 describes the outcomes of the various checks in [0047]-[0049] (emphasis added):

> [0047] The terms "freely operational" and "operating freely" are used herein to refer to the SCA operating such that the user is able to use the SCA as intended and free of any restrictions implemented by the test harness. …
>
> [0048] However, if the test harness restricts the use of the SCA, then the SCA is said to be prevented from operating freely. For example, in some instances, this may include disabling the SCA and preventing the SCA from being run on the UDPD. In some instances, this may include locking or disabling of one or more safety critical features of the SCA. In some instances, this may include permitting the SCA to run on the UDPD so that the user may still use non-safety critical features of the SCA but unable to use all safety critical features of the SCA. One or more checks on test harness 310 may be performed before SCA 304 is freely operational to provide a certain level of assurance that SCA 304 may operate properly on UDPD 200 before the user uses the safety critical features. Further, in some instances, one or more checks on test harness 310 may be performed during and/or after SCA is freely operational to provide a certain level of assurance that that SCA 304 continues to operate properly on UDPD 200.
>
> [0049] It should be appreciated that the term "permitting" is used broadly herein and may include allowing, enabling, unlocking, etc., in some instances. Further, it should be appreciated that the term "preventing" is used broadly herein and may include restricting, disabling, locking, etc., in some instances.

313. This is general teaching which applies to all the checks. Thus, if any check fails, the SCA may be prevented from operating freely. Preventing the SCA from operating freely may include disabling the SCA entirely or disabling one or more safety critical features while enabling use of non-safety critical features ([0048]).

314. The second point relates to the interaction between checks and between the installation and functional checks in particular:

> '[0060] A determination that SCA 304 operates properly on UDPD 200 may require specific outcomes for each check that is implemented. For example, in some instances, a determination that SCA is operating properly on UDPD requires an installation check to indicate that SCA is installed properly and also requires a functional check to indicate that SCA is functioning properly on UDPD 200. In some instances, a determination that SCA is operating properly on UDPD requires only functional check to indicate that SCA is functioning properly on UDPD 200 (e.g., if a proper installation has already been determined). A determination that SCA 304 is not operating properly on UDPD 200 may result, for example, from either a determination that

> SCA is not installed properly or a determination that SCA is not functioning properly. It should be appreciated that additional checks (e.g. host integrity check, coexistence check, interoperability check, power management check, and/or other checks not necessarily discussed herein) may also be implemented, with their specific outcomes also required for a determination that SCA operates properly on UDPD.'

315. **Installation Check**. This is covered at [0064] – [0067]. An Installation Check may be executed "to determine whether SCA 304 is installed properly on UDPD 200". This may involve, as an example, comparing (software) images of installed components of the SCA with reference installation data ([0065]). The reason for carrying out an Installation Check is, unsurprisingly, that "an improperly installed SCA compromises any assurance that the SCA is going to operate properly on UDPD". Importantly, EP223 explains that a successful Installation Check is not a guarantee that the SCA will operate properly: "… additional checks may be required before determining that the SCA operates properly on the UDPD". See [0064]. The specification continues:

> [0065] Installation check 412 compares the data for each installed SCA component against expected data associated with a proper installation (e.g., as defined by the reference installation data) to determine whether a proper installation has occurred. For example, a filename, CRC value, and/or version number associated with the installed SCA component may be compared with corresponding expected filename, CRC value, and/or version number in the reference installation data.
>
> [0066] If, for example, the image of one or more installed SCA components does not match the reference installation data, then installation check 412 indicates that SCA 304 failed to install properly on UDPD 200, which indicates that SCA 304 does not operate properly on UDPD 200. SCA 304 may then be prevented from operating freely on UDPD 200.
>
> [0067] If, for example, the image of each installed SCA component matches the reference installation data, then the installation check indicates that SCA 304 installed properly on UDPD 200 and one or more other checks (e.g., functional check, host integrity check, coexistence check, interoperability check, power management check, etc.) may be executed if required.

316. [0067] goes on to make clear that in certain instances, an exact match may not be required, where parameters and requirements encompass ranges and/or tolerances which allow for some deviation from an exact match.

317. For reasons which will become apparent, Dexcom were very keen to emphasise the many indications in the description that a check of whether the SCA is installed properly can only take place *after* installation. They also drew attention to Fig 3 which depicts three steps in the following order:

i) "*initial verification and validation testing"* performed on both SCA and test harness – this is explained to be "*performed by the manufacturer of the SCA 304 and test harness 310"* and is clearly distinct from any installation check;

ii) "install on UDPD"; and

iii) finally "*execute test harness",* which [0046] makes expressly clear is done "*after installation on UDPD"*.

318. Dexcom also drew attention to Figures 8 and 11 which are the flow diagrams illustrating the operation of installation checks in certain embodiments:

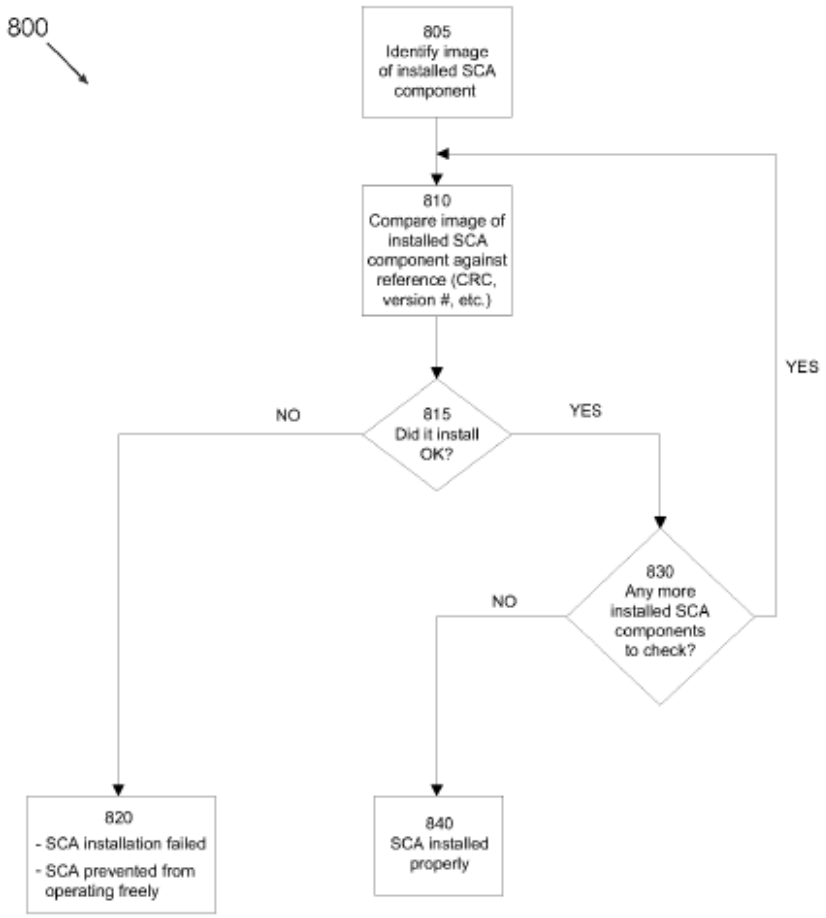


FIG. 8

319. Figure 8's process begins with "805 Identify image of <u>installed</u> SCA component", and the first decision box asks the past tense question "815 Did it install OK?", explained at [0136]: '… a determination is made as to whether the installed SCA component <u>was installed properly</u> or not". The outcome of a failed installation check should also be noted: the SCA is prevented from operating freely.

320. To the same effect, Figure 11's process begins with "1105 Install SCA & Test Harness on UDPD". The next step is "1110 Initiate Installation Check (e.g. compare installed SCA components against reference data)". The first decision box asks the same question as Figure 8: "1115 Did it install OK?" Fig 11 also shows the same outcome from a failed installation check.

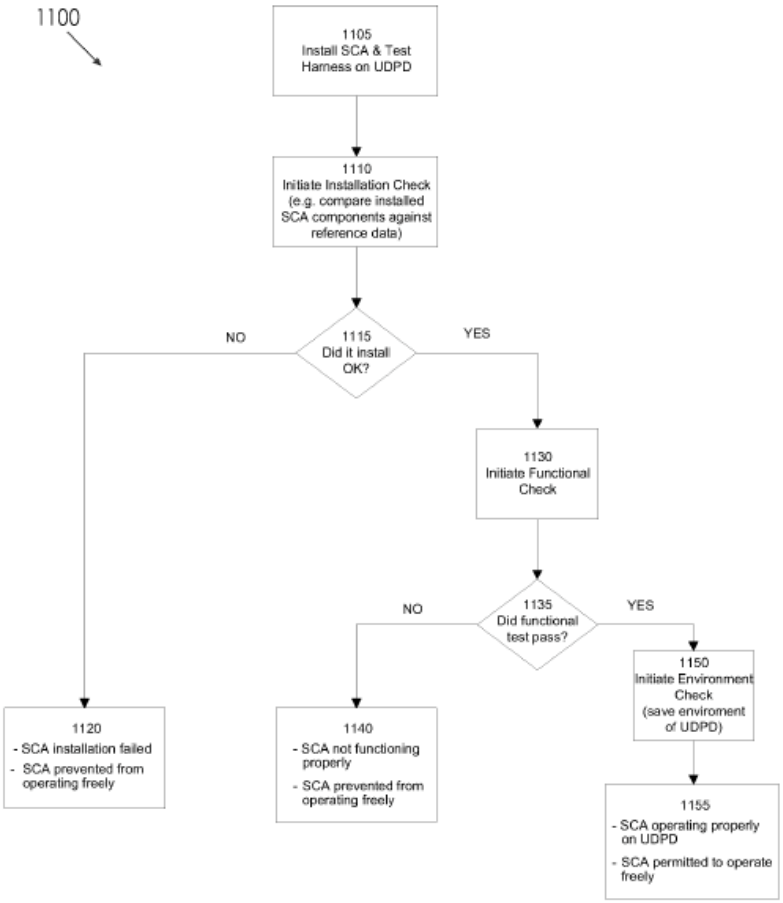


FIG. 11

321. Dexcom also draw attention to claim 2 which is dependent on claim 1, where it expressly refers to the installation of the SCA in the past tense: "…wherein the determining whether **the safety critical application (304) installed properly** on the uncontrolled data processing device (200) comprises…".

322. Dexcom also submitted that claim 1 does not seek to limit the way in which the "*determin[ation] … whether a safety critical application … is installed properly*" is carried out (there is, for example, no requirement that any particular technique be used). Neither does it require that whatever approach is chosen by the skilled addressee must provide complete assurance (or, indeed, any particular level of assurance) that the SCA is installed properly – this is clear from [0067].

323. **Functional Check**. This is covered at [0068] – [0070]. The objective is to check that the SCA "functions properly" on the UDPD: e.g. whether it can perform "calculations, measurements, etc." accurately, whether it "displays data properly", "whether it

communicates properly … with an external device", and whether it performs safety critical activities "in a proper amount of time". Various specific examples of functional checks are described in more detail ([0085] – [0109]), but a functional check is not said to be limited to these examples. It is suggested that one way to do this is to 'challenge' the SCA by getting it to perform calculations or measurements on 'reference computational input' – simulated data received from external devices such as external glucose monitoring devices is given as an example. You can then compare the results with reference data to see if the SCA is computing accurately on the UDPD [0089].

324. As Dexcom submitted, EP223 does not seek to limit the "*functional checks"* which may be performed, but it is clear that they must be checks which can identify defects in the ability of the SCA properly to perform its intended functions.

325. Dexcom also submitted that there is no limitation on the way in which the "*determin[ation of] … whether a safety critical application … functions properly*" in claim 1 is carried out, contending that it does not require that every aspect of the SCA's operation is checked, and does not require that the functional check provides any particular level of assurance that the SCA functions properly. I consider this follows from [0060] and also from the references in [0069] to a delay in performing an activity.

326. **Environment Check**. This is covered in particular at [0061] – [0063] and [0071] – [0075].

i) The reason for doing the check is that the operation of the SCA may be affected by its environment – i.e. the hardware or software configuration of the UDPD. If the SCA has been operating properly but the UDPD environment is changed, then this is a possible indicator that the SCA may not continue to operate properly. Of course, it is in the very nature of a UDPD that changes in hardware / software environment are to be expected; and there will be cases in which a change makes no difference at all to the operation of the SCA.

ii) The Environment Check is done "to determine a current environment of UDPD 200". It is not a direct test of whether the SCA is functioning properly, but rather a 'stocktake' which notes down the features of the "current environment – e.g. any currently installed software programs, applications drivers, hardware components, etc." (see [0176]). The features of the "current environment" can be "recorded at various times"; when the Environment Check is repeated subsequently, it can be determined (by comparison with the previously-stored "current environment") whether a change in the environment has taken place. [0073] explains "[i]f it is determined that the environment of UDPD 200 changes, then SCA 304 may potentially operate improperly on UDPD 200." EP223 envisages that, upon detection of a change in environment, further checks (e.g. a Functional Check) may be initiated to discover whether the change has compromised the proper operation of the SCA. Thus, detecting a change in the environment is not treated as detecting that something is wrong (in the way that a functional check does): it merely provides a reason to carry out a functional check. The point is particularly clear from figure 12, where the environment check happens in box 1220.

327. **Host Integrity Check**. This is covered at [0076]. This checks whether the integrity of the SCA *"has been corrupted"*.

328. **Coexistence Check**. This is covered at [0077] – [0081]. It is intended to address the situation where the UDPD "*hosts additional programs located on the device in addition to* SCA *304*", and particularly what EP223 terms "nonrelated" programs – those which do not "*work together with SCA 304 but may share resources with SCA 304"*. The Coexistence Check seeks to identify nonrelated programs which "*may not be able to coexist on UDPD 200 with SCA 304 without compromising a safety critical aspect of SCA 304, or operation thereof, on UDPD 200".*

329. **Interoperability Check**. See [0082]. This check anticipates the existence of programs which "*may interoperate with SCA 304 to provide functionality and capabilities to SCA 304,* referred *to herein as related programs"*. The idea is for the check to determine whether the "related programs" will interoperate properly with the SCA.

330. **Power Management Check**. This is covered at [0083] – [0084]. It seeks to determine that sufficient power is available for the SCA to operate properly on the UDPD.

331. A point arises on validity as to whether each type of check is separate and distinct: in other words, whether the same check can constitute both an installation check and a functional check or a functional check and an environment check. The categorisation of the various checks in EP223 is done by purpose, but I see no reason why a particular check might not fulfil more than one purpose. In my view, therefore, the Skilled Team would not read the various checks in EP223 as separate and distinct but instead, as capable of overlap.

332. As foreshadowed in the introductory paragraphs, EP223 seeks to implement various combinations of these checks in various specific ways with the objective of detecting and dealing with problems in the operation of the SCA. The rest of the description of EP223 is taken up with a more detailed description of various possible ways in which the checks can be deployed, with particular reference to the flowcharts in the figures. Some of these scenarios are the subject of the claims. These are discussed in more detail below in the context of claim construction.

333. Dexcom noted that EP223 contains very little (or no) information about how to actually implement the checks it describes. It is assumed that the reader will be familiar with the concept of performing checks on software and hardware and will know how to write code to do so. What is being presented to the reader as the invention is not the idea of performing software or hardware checks, but instead a variety of ways of combining and sequencing different kinds of checks together in order to address specific problems which may be encountered when running an SCA on a UDPD as illustrated in the various flowcharts contained in the figures.

Inventive concept

334. Dr Palerm described the inventive concept of claim 1 of EP223 as having two aspects:

i) first, to ensure that an SCA (such as the operating software for a CGM reader) continues to operate correctly in an uncontrolled, dynamic environment (specifically a mobile phone in the proposed amended claim) by performing the necessary testing on the uncontrolled device itself, rather than such testing of the software and its correct functioning being carried out by the manufacturer prior to release; and

ii) second, where a check fails, a user may be allowed to continue to access non-safety critical functionality while safety critical features are disabled.

335. Claims 7 and 9 add a mechanism for ongoing monitoring of the UDPD environment, with further checks performed when changes in the environment are detected.

CLAIMS / CONSTRUCTION

Claim 1

336. Claim 1 (including integer 1.5, which is proposed to be added by way of the conditional amendment) is as follows, in which I have underlined the expressions in issue:

1	*A method for hosting a safety critical application on an uncontrolled data processing device,*
1.1	*the uncontrolled data processing device being configured to permit a user to make software and/or hardware changes to the uncontrolled data processing device,*
1.2	*the method comprising:*
1.2(a)	*determining, with an uncontrolled data processing device, whether a safety critical application is installed properly and functions properly on the uncontrolled data processing device;*
1.2(b)	*preventing, with the uncontrolled data processing device, certain features of the safety critical application from operating on the uncontrolled data processing device upon verification that the safety critical application did not install properly or does not function properly on the uncontrolled data processing device,*
1.2(c)	*wherein the preventing comprises disabling safety critical features of the safety critical application from being executed on the uncontrolled data processing device and*
1.2(d)	*enabling non-safety critical features of the safety critical application to be executed on the uncontrolled data processing device; and*
1.2(e)	*permitting, with the uncontrolled data processing device, the safety critical application to operate free of any restrictions on the uncontrolled data processing device upon verification that the safety critical application is installed properly and functions properly on the uncontrolled data processing device,*
1.3	*wherein the safety critical application is a medically-related application and the uncontrolled data processing device is a wireless personal device comprising a display,*
1.4	*the uncontrolled data processing device being in data communication with at least one of an analyte monitoring device, a drug administration device, or a combination of both an analyte monitoring device and a drug administration device*
1.5	*wherein the uncontrolled data processing device is a mobile phone*

337. The claim is to a method of hosting an SCA on a UDPD (integer 1.1), wherein the method is for use with an analyte monitoring device and/or a drug administration device (integer 1.4). The experts focussed their evidence on the case of the UDPD being a mobile phone.

338. It is common ground that the claim contemplates that both an installation check and a functional check may take place (integer 1.2(a)).

339. The consequence of a failed check is described in integers 1.2(c) and (d). It is that safety critical features of the SCA are disabled (integer 1.2(c)) while non-safety critical features of the SCA are enabled (integer 1.2(d)). Abbott characterised this as "**selective enablement**".

340. The patent contemplates that selective enablement may take place in different ways. The claims however relate to the selective enablement of safety critical features of applications which are (taken as a whole) safety critical applications, but which include both safety critical and non-safety critical features.

341. The following construction issues arise, in which, in the usual way, the arguments were influenced by the parties' positions on validity and infringement.

'Safety critical application'

342. Dexcom submitted that the meaning of this term is apparent from [0001]: "[s]afety critical systems are systems whose failure or malfunction may result in significantly detrimental consequences such as death or injury to persons, severe damage or loss to equipment or to environment." As further explained in [0003] "[m]edical systems are an example of safety critical systems that require a certain level of confidence that the system will operate and continue to operate properly. Medical systems may detrimentally affect a user's health and well- being if not operating properly or not known to be operating properly. This is especially true for medical systems that provide user's [sic] with health-related diagnostic or therapeutic information."

343. Accordingly, Dexcom invited the conclusion that a "safety critical application" is a software application whose failure or malfunction may result in significantly detrimental consequences such as death or injury to persons, severe damage or loss to equipment or to environment.

344. Abbott's argument on the interpretation of this term started from [0001], but then focused on some evidence from Dr Stirbu concerned with the Gejdos prior art (which I discuss below). Abbott were critical of Dr Stirbu's evidence, saying he took too expansive a view. That segued into this submission:

> 'The "*consequences*" referred to in the definition of SCA are clearly intended to be much more direct than that. An SCA is an application which is *directly* involved with monitoring and treating the patient or recommending that the patient take action, such that malfunction would have a *direct* effect on the patient, e.g. an application controlling an analyte monitoring device and/or a drug administration device, which are specifically referred to in integer 1.4.'

345. In this submission, Abbott are trying to write additional limitations into this expression. In my view, the proper interpretation of this term is straightforward, and I agree with the conclusion invited by Dexcom.

346. The final point to make concerns the breadth of the expression. EP223 speaks of safety critical systems (i.e. hardware and software) but the claim requires a safety critical application (expressed in software). However, in view of the way the claim is drafted, with much non-limiting language, I see no reason why an SCA should be limited to actual executable code. A purposive interpretation indicates that any software whose failure or malfunction may result in significantly detrimental consequences such as death or injury to persons etc. falls within this expression.

Integers 1.2(b) – (d) individually

347. The dispute over the proper construction of integers 1.2(b) – (d) concerns infringement. Abbott chose to address these integers compendiously, whereas Dexcom addressed them in parts. I will examine the parts first and then consider Abbott's compendious arguments. These integers (with 1.2(e)) comprise the steps in the method of claim 1. There are basically two steps: the determination/verification step which dictates the outcome: preventing or permitting.

"determining … whether a safety critical application is installed properly … on the uncontrolled data processing device" – integer 1.2(a) (1st part)

348. Dexcom emphasised the use of the present tense in this integer, contending that a determination of whether the SCA is installed properly is expressly called for. They submit the purpose of this check is clear – the process of installing an application on a UDPD may not be executed correctly; and if the SCA is not installed properly then its operation may pose a risk to the user. A check of whether the SCA is installed properly can only happen after installation of the SCA has taken place.

349. For their part, Abbott pointed out the check is whether the SCA is installed properly, not 'has been'. This, in my view, is meticulous verbal analysis which takes no account of the technical reality.

350. I agree that the description of EP223 contains numerous confirmations, express and implicit, that installation checks are checks performed after installation of the SCA has taken place, in order to verify that installation took place successfully. I also agree that it does not make technical sense to speak of an installation check carried out *before* installation. A check before installation may check the integrity of the software to be installed, but it cannot check whether the actual installation has occurred properly.

"determining … whether a safety critical application … functions properly … on the uncontrolled data processing device – integer 1.2(a) (second part)

351. I agree this corresponds to EP223's description of the functional check(s).

352. Dexcom argued that to constitute a 'functional check', the check must be a *direct* check of the SCA's ability to perform its intended functions and not an *indirect* check. The arguments on this point were made by Dexcom in the context of infringement. Furthermore, it is one of those points which is really only comprehensible once the infringement issue is understood. For that reason I will deal with it under infringement, even though it seems to me the argument raises an issue of the proper interpretation of this integer and in particular, whether a time check constitutes a determination of whether a SCA functions properly.

"preventing … certain features of the safety critical application from operating … upon verification that the safety critical application did not install properly or does not function properly on the uncontrolled data processing device" – integer 1.2(b)

353. The principal issue arose on this integer, but it is convenient to come back to it once I have addressed the remaining integers.

"wherein the preventing comprises disabling safety critical features of the safety critical application … and" – integer 1.2(c)
"enabling non-safety critical features of the safety critical application …" – integer 1.2(d)

354. Although split into two integers, in fact this is a single integer concerned with the scope of the 'preventing'. The "*preventing*" is a selective "*preventing*", in which some features (safety critical) of the SCA are *disabled* (integer 1.2(c)) but other features (non-safety critical) are *enabled* (integer 1.2(d)).

355. Dexcom pointed to the view expressed by Dr Palerm to the effect that he considers that provided that failure of <u>one</u> of the installation or functional checks can result in the selective disablement of safety-critical features of the SCA, it will be sufficient to satisfy the requirements of the claim if failure of the other check can only ever result in *total* disablement of the SCA. Dexcom submitted that the claim is simply not concerned with any mechanism of triggering total disablement of the SCA; to the contrary, integer 1.2(d) makes expressly clear that the "*preventing*" referred to in integer 1.2(b) actually comprises <u>enabling</u> non-safety critical features of the SCA: it could not be clearer that the total disablement of the features of the SCA is not something which can satisfy integer 1.2(b)'s "*preventing*" requirement.

356. This argument arises in particular from this situation: what if the SCA has no non-safety critical features? Can the claimed method still be used if the preventing comprises disabling the SC features of the SCA but there are no non-safety features which can be enabled? I return to this issue in the compendious section below.

"permitting … the safety critical application to operate free of any restrictions on the uncontrolled data processing device upon verification that the safety critical application is installed properly and functions properly on the uncontrolled data processing device" – integer 1.2(e)

357. Dexcom submitted that the same points made in relation to integer 1.2(b) above apply. Here the importance of the two-input "*verification*" step is again highlighted – the system needs to be satisfied that <u>neither</u> the installation check <u>nor</u> the functional check referred to in integer 1.2(a) has failed before it will permit the SCA to operate freely.

Integers 1.2(b) – (d) compendiously

358. Abbott stated their position as follows:

i) Integers 1.2(b) – (d) together require that, where it is determined that the SCA did not install properly <u>or</u> does not function properly, certain features are prevented from operating, wherein "*preventing*" comprises what Abbott called "selective enablement".

ii) So the method must include the capability to undertake an installation check (or checks) and a functional check (or checks); and the outcome of a failed installation check or failed functional check must comprise selective enablement.

iii) However, it is not a requirement that both the functional check and the installation check have this result. Integer 1.2(c) states that the preventing "*comprises*" selective enablement. It is not a requirement that a functional check must take place when, for example, an installation check has shown that the software is not installed.

iv) So, the claimed method provides for undertaking both types of checks even if not every situation will require both, and if the result of at least one of those checks is selective enablement in accordance with integers 1.2(c) and 1.2(d), the claimed method is being performed.

359. Abbott point to the argument presented by Dr Stirbu and Dexcom that the claims require that the outcome of a failed installation check is (and is always) that the SCA is selectively enabled – i.e. despite a failed installation, some features of the SCA must be enabled in all cases. Abbott submit that this makes no sense from a technical perspective. In particular, it would not make sense to require that the outcome of a failed installation check in every case is that at least some features of the SCA continue to be enabled. In many if not most cases, if the SCA does not install, then it will not be able to operate at all, as Dr Palerm said. Dr Stirbu agreed with this as a technical matter.

360. Abbott also contended that Dexcom's approach would be inconsistent with [0137] of EP223, describing an embodiment (emphasis added):

> [0137] If, for example, the image of the installed SCA component does not match the reference installation data, then it is determined that SCA 304 failed to install properly on UDPD 200, as represented by block 820. SCA 304 may then be prevented from operating freely on UDPD 200. Again, in some instances, this may comprise disabling the SCA so that it is unable to be run on the UDPD. In some instances, this may comprise permitting the SCA to operate so that the user may still use non-safety critical features of the SCA but unable to use the safety critical features.

361. Abbott suggested this passage describes two things which can be done when the installation check is failed: either disabling the SCA completely, or only partially (i.e. selective enablement). They say it would be perverse to construe claim 1 as covering only one of those options (especially if that is the latter option, which is not technically sensible/feasible in some cases, referencing their point recorded in paragraph 359 above).

362. Abbott's final point was that claim 1 is a method claim. If (for example), the system performs an installation check (which is passed) and then a functional check (which is failed), and then selectively enables the SCA in consequence of the latter, then that would be a use of the claimed method. Abbott submitted that example is sufficient for their infringement case.

363. Dexcom attacked Abbott's reliance on [0137], saying Abbott depended on a bizarre reading of that paragraph. However, [0137] is clear. The far better point made by Dexcom was that it could not be assumed that claim 1 covered everything described in the specification or [0137].

364. As for Abbott's perverse argument, Dexcom made three responses:

i) If partial disablement is unfeasible "*in some cases*", then *in those cases* something else will be done and the claim will not be infringed – there is no need to disapply the clear language of claim 1 to force it to apply in every conceivable case.

ii) Matters might be otherwise if the Skilled Addressee would understand partial disablement to be unfeasible in all cases, but there was no evidence that this would be so. Quite the contrary: Dr Stirbu explained in his cross-examination that, while app installation is a tightly-controlled process on some platforms (such as iOS devices, in which partial disablement following the failure of a signature check is agreed not to be feasible), in other UDPD contexts (for example, PCs running Windows) a developer can have a much greater level of control over the installation process.

iii) While, perhaps, the proposed amendment to claim 1 is intended to strengthen Abbott's position in this respect – to support the submission that the skilled addressee would think that partial disablement upon installation failure in the context of a mobile phone app could not have been what was intended – in fact it does no such thing, since the amended claim encompasses any kind of mobile phone running any kind of operating system (including operating systems without strict pre-installation checks).

365. Accordingly, there is nothing perverse about giving effect to explicit limitations in the claim.

366. Dexcom characterised part of Abbott's argument in this way: Abbott says that it does not matter if only the failure of the functional test can ever have the consequence of selective disablement, provided that the failure of the installation will result in total disablement.

367. As Dexcom submitted, the reality is that, while the description of EP223 (and, particularly, [0137]) contemplates two options upon the failure of the installation check – total disablement, or partial disablement – claim 1 claims only one of those options. Dexcom submitted that this is an entirely unremarkable result: the disclosure of the specification of a patent is frequently broader than its claims – for example because the patent was amended during prosecution, which is, in fact, what happened here: claim 1 of EP223 as filed requires that the SCA is prevented from "*operating freely*" upon failure of the installation check. Claim 3 of EP223 as filed limits that prevention to selective disablement of safety critical features. Claim 1 of EP223 as granted corresponds to claim 3 as filed.

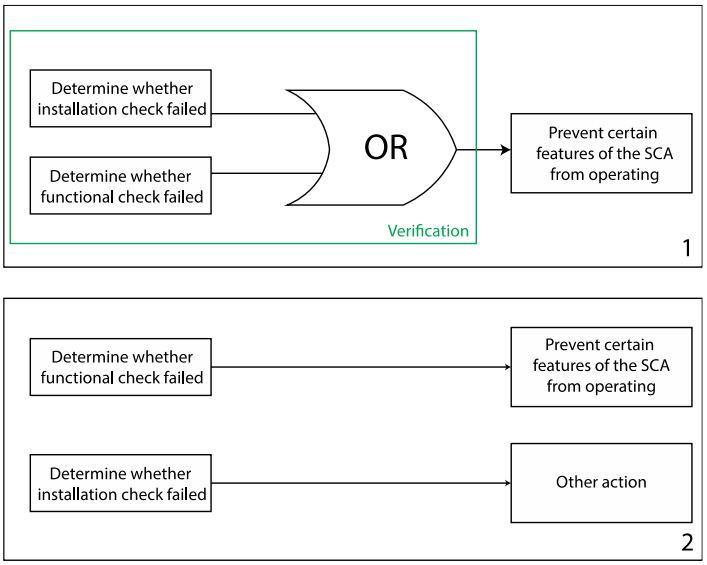
"preventing … certain features of the safety critical application from operating … upon verification that the safety critical application did not install properly or does not function properly on the uncontrolled data processing device" – integer 1.2(b)

368. I return to Dexcom's arguments on this integer. Dexcom submitted as follows:

i) this integer requires a "*verification*" that the installation check or the functional check have failed, in which case "*certain features*" of the SCA are prevented from operating. Action is then taken "*upon*" that verification.

ii) Clearly, the references to verification of the safety critical application "*not install[ing] properly*" or not "*function[ing] properly*" require consideration of the outcomes of the "*determinations*" required in integers 1.2(a), *i.e.* the 'installation check' and the 'functional check'. A further or additional "*determination*" not previously referred to in the claim cannot be considered in the "*verification*" instead of one (or both) of the previously-referenced installation / functional checks.

iii) The "*verification"* must involve consideration of the results of the installation and functional checks referred to in integers 1.2(a) and (b). In logic terms, it requires an "OR" gate. The required "*verification"* will not occur if only the result of one check – installation or verification – is considered when deciding whether to trigger the "*prevent[ion] … of certain features of the SCA from operating"*. This is illustrated in the following diagrams – the necessary "*verification*" takes place only in the upper box (1):



iv) The lower box (2) does not contain the necessary "verification" step. It would not make sense for the patentee to have specified:

a) two distinct safety tests; and

b) one action to be taken in consequence of either of the safety tests failing;

yet have intended the claim requirements to be satisfied by the use of a system in which the result of only one safety test is ever considered when deciding whether or not to take the action. Clearly, the patentee has included two distinct safety tests in order to build up two distinct layers of safety, and both must therefore be taken account of in the "*verification*" step. If the steps in the

lower box (2) constituted "*verification*", then one of the safety tests specified earlier in the claim would be entirely redundant.

Discussion

369. In my judgment, although each side's argument includes points with some merit, neither side's argument is entirely correct.

370. As indicated above, Dexcom commended their OR gate logic. However, I am not at all sure they really meant OR gate logic. If the inputs are 1=pass and 0=fail and the outputs are 1=operates freely and 0=selective enablement, an OR gate would result in selective enablement only if both checks failed. In all the other three instances, the app would operate freely, which does not accord with reality or the claim.

371. It seems to me that the better analogy is an AND gate, where it is only if both checks pass that the app is permitted to operate freely. In the other three instances, selective enablement is the result i.e. if both checks fail or if one or the other fail.

372. Abbott argue that this would produce a perverse result i.e. that it would be perverse to construe the claim as requiring selective enablement if the app fails the installation check. But this argument, it seems to me, requires a hindsight approach to interpretation of the claim. The sleight of hand in this argument is to invite the claim to be viewed through the eyes of someone familiar with how smartphones operated in 2009. In that world, if an app failed an installation check then the app would either not be installed at all, or it would not be allowed to run. But that is plainly not the right approach to EP223 which does not acknowledge either the existence or functionality of 2009 smartphones. To the contrary, EP223 it seems to me explicitly contemplates SCAs which have both safety critical features and non-safety critical features. Once that is kept in mind, it is entirely logical to have selective enablement (of the non-safety critical features) whilst the safety critical features are disabled on the occasion of an app failing an installation check.

373. It also assists to have in mind the various possible routes through the steps contemplated in claim 1, where completion is signified by 'End' and a further step by →:

i) The SCA fails the installation check and cannot operate at all. No selective enablement is possible. End.

ii) The SCA fails the installation check, but some non-safety critical aspects of the SCA are able to operate and are selectively enabled. →

iii) The SCA passes the installation check. →

The functional check cannot be performed in scenario i) but it can in scenarios ii) and iii) which means:

iv) Following scenario ii), the selectively enabled non-safety critical aspects of the SCA fail the functional check and are disabled. No part of the SCA is permitted to operate. End.

v) Following scenario ii) the selectively enabled non-safety critical aspects of the SCA pass the functional check and are or continue to be selectively enabled. End.

vi) Following scenario iii), the SCA fails the functional check such that no part of the SCA is allowed to operate. End.

vii) Following scenario iii), the SCA fails the functional check, but some non-safety critical aspects of the SCA are able to operate and are selectively enabled. End.

viii) Following scenario iii), the SCA passes the functional check and the SCA is permitted to operate freely. End.

374. With these complete routes in mind, it seems to me that the claimed method includes viii), vii), v) and ii) but not i), iv) or vi), since the claim requires either complete or selective enablement. I remind myself that to infringe, it is not necessary that the claimed method is used all the time – it is sufficient if it is used some of the time.

375. The key here is to focus on the distinction clearly drawn in the Patent and in claim 1 between:

i) the SCA operating free of any restrictions (on verification that the SCA is installed properly and functions properly on the UDPD).

ii) 'preventing' the SCA from operating freely. The point being that the Patent contemplates a range of possibilities in this 'preventing'. Claim 1 however does not claim the whole range of possibilities. Integer 1.2(b) on its own, would cover a range of possibilities, but the patentee explicitly included a further limitation in integers 1.2(c) and (d), where the 'preventing' is limited to this 'selective enablement'.

376. The consequence is, in my view, that if this 'selective enablement' is not possible either because of i), iv) or vi) above, then the claimed method is not used.

377. One final issue remains and that is Abbott's argument that this is a method claim (see their argument at paragraph 362 above). Taken to its logical conclusion, on this argument this claim would be infringed even if no selective enablement was possible at all e.g. if an app passed both an installation check and a functional check, and the app was permitted to operate freely. Thus, it seems to me that the only possible conclusion is that in an implementation of the claimed method, the implementation must be *capable* of selective enablement if an installation check fails OR if a functional check fails.

378. In case I am wrong in that conclusion, I will also proceed to consider infringement and validity on this alternative construction, where, if an implementation produces a result which matches at least one of the four outcomes contemplated in the claim (but not all of them), then that is a use of the claimed method. It may be noted that this makes the claim extremely broad.

Claims 7 and 9

379. Claims 7 and 9 go together because they claim the environment check (claim 7) and the ensuing functional check that is carried out if a change in environment is detected (claim 9). The integers of these two claims are as follows:

7	*The method of any of the preceding claims, comprising:*
7.1	*identifying, with the uncontrolled data processing device, a first current environment of the uncontrolled data processing device, the first current environment associated with a time when safety critical application is permitted to operate on the uncontrolled data processing device;*
7.2	*identifying, with the uncontrolled data processing device, a second current environment of the uncontrolled data processing device, the second current environment associated with a time after the safety critical application is permitted to operate on the uncontrolled data processing device;*
7.3	*comparing, with the uncontrolled data processing device, the second current environment with the first current environment; and*
7.4	*determining, with the uncontrolled data processing device, whether an environment change has occurred.*

9	*The method of claim 7, comprising:*
9.1	*determining, with the uncontrolled data processing device, whether the safety critical application functions properly on the uncontrolled data processing device after a determination that a change in environment occurred;*
9.2	*preventing, with the uncontrolled data processing device, certain features of the safety critical application from operating on the uncontrolled data processing device when determined that safety critical application does not function properly on the uncontrolled data processing device after the determination that the change in environment occurred; and*
9.3	*permitting, with the uncontrolled data processing device, the safety critical application to operate free of any restrictions on the uncontrolled data processing device when determined that safety critical application functions properly on the uncontrolled data processing device after the determination that the change in environment occurred.*

380. It is convenient to use the shorthand ‘environment check’ for integers 7.1-7.4 but it is necessary to keep the four steps in mind.

381. Although Dexcom presented a detailed analysis of all these integers in their opening, I did not detect that any issues of construction arose. However, in their closing, Dexcom raised an argument that what Abbott relied upon as constituting the environment check (repetition of the time check) could only result from an absurd construction of claim 7. The problem with this argument is that if repetition of the time check results in a

determination within integer 7.4, then the four steps in claim 7 are present. What the infringement point (which I consider below) illustrates is the breadth of the claim.

382. Dexcom also relied on evidence from Dr Stirbu as to what would normally be understood as an environment check: that an environment check would only be carried out once a functional check had been passed, and would involve checking whether hardware, drivers, OS etc of the device met the minimum requirements to run the application and then monitoring for changes. However, 'environment check' is not a term of art and is not used in the claims in any event.

383. The structure of claims 7 and 9 make clear that, as mentioned above, a change in environment does not automatically lead to selective enablement. As claim 9 provides, a functional check is initiated upon a determination (in accordance with claim 7) that a change in environment has occurred. That functional check can lead to selective enablement (integers 9.2 and 9.3).

384. In combination, claims 7 and 9 thereby provide for ongoing monitoring on the SCA, whereby whenever a change in environment is detected (e.g. if the user updates the OS on their UDPD), the device will initiate a functional check to ensure the SCA can continue to operate correctly in that new environment.

INFRINGEMENT OF EP223

385. The G6, G7 and D1 systems are all alleged to infringe EP223, but only when used with a smartphone app (not the dedicated reader). Dexcom acknowledged there are some differences between these three systems. Abbott addressed the G6 and Dexcom the G7, but by the time of closings, neither side contended that any of these differences were material.

386. Abbott contended that the disputes on infringement principally turn on claim construction, identifying three issues on claim 1:

i) Whether the installation process of the G6 meets the requirements of an "*installation check*" of integer 1.2(a).

ii) Whether the "*time check*" on the G6 device meets the requirements of the "*functional check*" of integer 1.2(a).

iii) Whether these checks in combination meet the requirements of "*preventing*" in integer 1.2(d).

'installation check'

387. The PPD makes clear that installation of the G6 App is subject to a digital signature check which is performed by the iOS and/or Android operating system when the G6 App is downloaded onto a user's device. When the app is downloaded, iOS (or the Android Play Store in the case of an Android phone) checks the digital certificate of the app to confirm that it has been verified and that the downloaded file has not been modified. If the verification check fails, the app will not install.

388. Abbott contended that this verification step is part of the process of checking that the application is correctly installed. Thus it comprises "*determining ... whether the safety critical application is installed properly*" as required by integer 1.2(a).

389. Abbott relied on the following parts of Dr Stirbu's evidence: (footnotes omitted), in support of their submission that an installation check in accordance with the claim was carried out:

> 57. For mobile applications, various techniques to verify the integrity and authenticity of apps were already known and being used in 2009. The most common examples at the time (and still is to this day) were digital signatures and certificates, which were routinely used, including by the Apple and Google, to verify the integrity and authenticity of applications. Specifically, both the iOS (Apple) and Android (Google) were using digital signatures to verify the integrity of app installation packages and to confirm that the app had installed correctly on the mobile device – this feature was included in iOS since the release of iOS 2.0 in 2008 and in Android since its initial release in 2008.
>
> …
>
> 60. In iOS, a similar digital signature check is performed each time a user launches an app. The same digital signatures described above are used to verify that the installed app files are correct and have not been modified, prior to launching the app.

390. However, it is necessary to read [57] in combination with [59] in particular, where Dr Stirbu made it clear the digital signature check is performed *before* installation begins (emphasis added):

> 59. In essence, the digital signatures (from the developer and from Apple or Google) confirm that (i) the app has been verified by Apple (or Google), (ii) the app was created by a known sender (the developer), and (iii) that the files in the installation package have not been modified/altered in transit, <u>before beginning installation</u>. In effect, the digital signatures are a promise by Apple (or Google) that "yes, this person (the developer) is who they say they are, and we, Apple (or Google), certify that".

391. In my judgment this digital signature check is not an installation check within claim 1.

392. However, Abbott also sought to argue that the digital signature check which is performed in iOS each time an app is launched constitutes an installation check within claim 1. Dexcom objected on the basis that this argument nowhere appears in Abbott's Statement of Case on Infringement ('SOCI') and no application was made to amend. Accordingly, Dexcom did not address this argument.

393. I agree that this point does not feature anywhere in Abbott's (Amended) SOCI of EP223. If this point had been pleaded, I would have found that this constituted an 'installation check'. Abbott were well aware of this pleading objection in opening and failed to do anything about it. Accordingly, Dexcom's objection is valid.

'functional check'

394. The functional check relied on for the purposes of the infringement case is a check referred to in the evidence as the "**time check**".

395. The G6 system performs several checks designed to "*ensure that the G6 App is able to operate*". As set out at ¶45 of the PPD under the heading "*Maintaining Operational State*", there are several requirements that the G6 App is required to meet (emphasis added):

> (a) The database must be operational;
>
> (b) There must be sufficient disk space to store information;
>
> (c) The environment that the app is running in must be a known compatible environment (i.e. through the Compatibility Check described above);
>
> **(d) The app must maintain a valid reference to time**; and
>
> (e) The app must be running.

396. These requirements are said to be "*monitored continuously*" by monitoring the status of critical elements of the G6 App and "*managing any errors encountered*". (The same checks are performed by the D1 and G7 systems, with some additional checks performed on the G7).

397. The requirement in (d) that the app "*maintain a valid reference to time*" is what is referred to as the "**time check**" in the evidence. It is described in more detail at ¶50 of the PPD:

> User action, such as changing the time in the phone settings, can lead to the G6 App losing track of time. This can lead to past glucose measurements appearing to have been made in the future. Where the G6 App determines that this has happened, the EGV and trend graph displays are replaced with a "Adjusting Clock" message (as shown on the below), which is displayed until phone time has moved past the timestamp of the most recent glucose measurement (i.e. no glucose measurements appear to occur in the future). During this period, the user may access other app functions.

398. On this basis, Abbott submitted that the time check is therefore a "*functional check*" within integer 1.2(a), for the following reasons:

i) The time check includes a determination of whether the G6 App is functioning properly, for as the PPD explains, it will not function properly if it loses track of time. In other words, the G6 App determines whether, having regard to time reference, it is able to function properly (as accepted by Dr Stirbu).

ii) It does so in the same way as functional checks are said to operate in the specification of EP223, namely by continuously monitoring the time synchronisation of the G6 App to determine whether it is maintaining a valid reference to time.

399. If the time check determines that the G6 App is not functioning properly in this respect, the result is that an error message is triggered and display of glucose data is prevented.

Other functionality of the app can continue to be used, however (e.g. looking at historical glucose data). Thus the time check also satisfies the requirements of integer 1.2(b) – (d).

400. Dr Stirbu said in his written evidence that the time check cannot be a functional check because it does not check whether the app performs calculations correctly, displays data properly, communicates properly with an external device or performs safety critical functions in a proper amount of time. It only checks whether a change to the phone settings has affected the local time recorded on the phone when compared to a reference time server. In his view, the Time Check does not determine if the app functions properly. The Time Check responds to a user change to the phone settings (i.e. changing the phone clock), but assumes that the app is functioning correctly, as such it is not a functional check.

401. Abbott characterised Dr Stirbu's evidence as him saying the time check is not one of the specific examples of functional checks mentioned in EP223. But, as Abbott submitted, these examples are not suggested to be limiting in the description, nor are the claims limited to specific kinds of functional check. The patentee has simply put forward several examples of the kinds of test that may be performed to determine if an SCA continues to function properly, but has not suggested that they are exhaustive.

402. These points notwithstanding, as mentioned above, Dexcom argued that to constitute a 'functional check', the check must be a *direct* check of the SCA's ability to perform its intended functions and not an *indirect* check. Dexcom argue that EP223 deals with issues which may *indirectly* affect an SCA's functionality by way of a host of checks which are quite distinct from the functional check: the installation check, the environmental check, the host integrity check, the coexistence check, the interoperability check, and the power management check.

403. In his written evidence, Dr Stirbu characterised the time check as most similar to an Environment Check of EP223, in that the purpose of the checks is similar – they determine whether the current environment has changed. He also pointed out that the Environment Check and the time check can only be performed when the app is functioning properly.

404. Dexcom also relied on [0068], but this just lists examples and is not limiting:

> [0068] Functional Check – In some aspects of the present disclosure, a functional check 414 may be executed to determine whether SCA 304 functions properly on UDPD 200. For example, functional check 414 may check whether SCA 304 performs computations (e.g. calculations, measurements, etc.) accurately on UDPD 200; whether SCA 304 displays data properly on a display of UDPD 200; and/or whether SCA communicates properly via UDPD with an external device; and/or whether SCA 304 performs these and/or other safety critical activities in a proper amount of time.

405. Dexcom acknowledged that EP223 refers to 'timing test routines' in [0092-3] as possible functional checks, but they contend that these are *direct* tests of the SCA's

ability to perform "activities (e.g. computations, communications, etc.) on UDPD 200 in a timely manner-e.g. within times falling within predetermined parameters…".

406. In his oral closing, Mr Brandreth KC submitted that a check on the system time is just that, but it is not a check on the functionality of the software. The software works exactly as designed if the time is wrong, but he was constrained to accept that the information the app outputs may not be accurate.

407. In my view, Dexcom's argument is an attempt to write an additional limitation into the claim to the effect that the check must be a *direct* test of whether the SCA functions properly. It seems to me there is no support for this in the specification and this element of the claim (like many others) is expressed broadly. On this basis, the time check constitutes a functional check.

Selective enablement

408. If the digital signature check fails, the app will be prevented from launching (or installing), so no part of the app is enabled. This is scenario i) above and not within the claimed method.

409. If the digital signature check passes and if the time check passes, the SCA is permitted to operate freely (in accordance with integer 1.2(e)). If the digital signature check passes, but if the time check determines that the G6 App is not functioning properly in this respect, the result is that an error message is triggered and display of glucose data is prevented. Other functionality of the app can continue to be used, however (e.g. looking at historical glucose data). Thus, assuming I am correct in my finding that the time check is a functional check, it results in selective enablement. This is scenario vii) above and prima facie within the claimed method.

410. However, if my conclusion on construction is correct (see paragraph 377 above), Dexcom do not infringe.

411. On the alternative construction (see paragraph 378 above), Dexcom would infringe.

The finding of no infringement by the Mannheim Court.

412. Finally, Dexcom invited my attention to the way in which the Mannheim Court found no infringement. There were two points. The first was that the installation check relied upon took place prior to installation and therefore could not constitute an installation check. They pointed out that a successful (pre-)installation check would merely be a condition for the installation to be allowed to commence and would not preclude the possibility of errors occurring during the installation process itself or detect any errors if they did occur.

413. I have reached the same conclusion as the Mannheim Court, the result being that Abbott's infringement case as pleaded, must fail.

414. However, I will briefly address the unpleaded allegation that digital signature checks which are carried out each time the app is launched occur post-installation and constitute installation checks within claim 1. As far as I can see, this further allegation was not considered by the Mannheim Court. Even if these are considered to be

installation checks within claim 1, the infringement case still fails for the second reason identified by the Mannheim Court. This is that the installation check(s) relied upon did not result in selective disablement of safety-critical features of the SCA. Again, I have reached the same conclusion.

Claims 7 and 9

415. Abbott's argument for infringement of these claims was as follows. They contended that the time check also comprises an environment check of claim 7. The time check necessarily involves a determination of whether there has been a change in the operating environment of the G6 App – namely that the device has lost time synchronisation. The consequence of this is a determination that the G6 App no longer functions properly (e.g. past glucose measurements will be associated with the wrong time), which fulfils the requirements of a functional check. So, although it is described in the PPD as if it were a single process, the time check in fact comprises the two checks required by claims 7 and 9.

416. Dr Stirbu agreed that the time check "*if anything, is most similar*" to the environment check of EP223, but gave two reasons why, in his view, it is not an environment check within the meaning of the claims, neither of which in my view carry any weight:

i) The device time "*does not affect the capabilities* [of the device]". Abbott submitted this was obviously technically wrong (since the device time is used for core functions of the app such as recording historical data and reporting current EGVs) and also irrelevant (since nowhere does EP223 define the environment in such terms).

ii) The device time "is not at all similar to the examples given in EP223 of components of the current environment." Abbott did not agree but said this cannot be determinative since the examples are only examples and not exhaustive.

417. Dexcom took another pleading point on infringement of claim 7, contending in closing that it appeared (from Dr Palerm's evidence in cross-examination) that Abbott's case may actually be that the environment check is not the time check itself but the underlying process which triggers the repetition of the time check, a case which Dexcom contended was not open to Abbott.

418. This argument demonstrates the danger of relying too heavily on 'environment check' as a precis of the claim. Abbott's SOCI makes it clear that Abbott rely on a time check for integer 7.1 and a time check for integer 7.2, a comparison between the two resulting in a determination of whether an environment change has occurred.

419. Dexcom also argued that a time check is just a time check and involves no identification of environments, no comparison and no action taken on the basis of any comparison. This argument carries no weight, in view of the pleaded case which in my view demonstrates that if the Dexcom devices infringed claim 1, they would also infringe claims 7 and 9.

420. In relation to the infringement arguments, Dexcom also raised a Gillette defence but consideration of this must await the validity analysis.

VALIDITY: NOVELTY

Gejdos

Introduction

421. In closing, Dexcom made it clear that it maintained the novelty attack based on Gejdos as a squeeze on infringement. Dexcom accepts that the database integrity check in Gejdos is not a *direct* check of the functionality of the application. Therefore, on Dexcom's construction of integer 1.2(a), Gejdos does not disclose a functional check. Since I have found against Dexcom on construction, I must assess whether Gejdos discloses a functional check and all the other elements of the claim.

Disclosure

422. Gejdos is a US patent application published on 11 June 2009 titled "*System and Method for Database Integrity Checking*". It claims and discloses a method for checking the integrity of a database containing physiological information, the database being accessible by a healthcare management software system ('HMSS').

423. The database includes a patient's (or patients') healthcare related information – for example, blood glucose values [0027]. [0028] says:

> [0028] Healthcare management software system 106 includes instructions which when executed by computing device 100 present physiological information 110 or information based on physiological information 110 to an output device 112. Exemplary information presented by healthcare management software system 106 to output device 112 include diaries of blood glucose values and reports showing a plurality of blood glucose values. Exemplary reports include standard day reports wherein the blood glucose values are grouped according to the time of day taken, standard week reports wherein the blood glucose values are grouped according to the day of the week taken, trend graphs to illustrate temporal trends in blood glucose values, and other suitable reports.

424. The HMSS can be run on *e.g.* a "*cellular device*" or "*personal digital assistant 'PDA' such as BLACKBERRY brand devices*" [0025].

425. The performance of "integrity checks" (which may be "*any process whereby the accuracy of the patent database 104 may be affirmed or denied"* [0043]) of the patient database in the HMSS at various times is described, for example when the HMSS is installed or when the HMSS is launched. This is clearly shown in Fig 4:

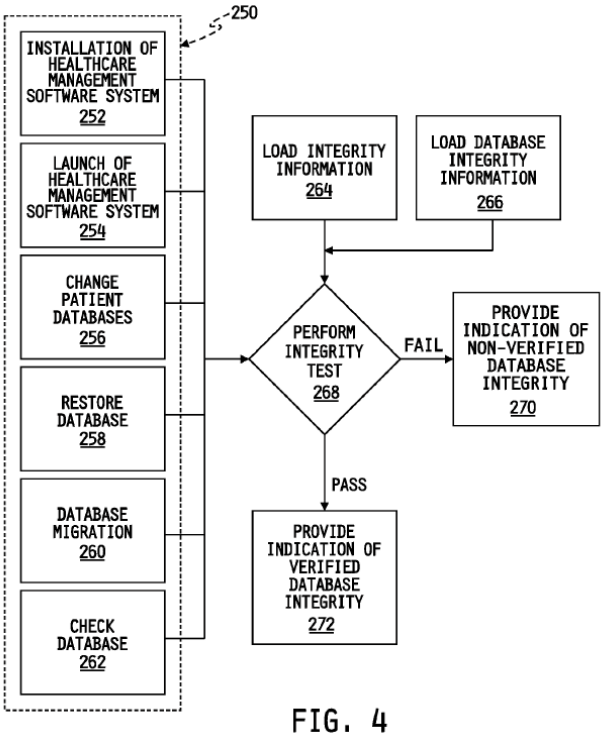


FIG. 4

426. Dr Stirbu considered that all of the features of claim 1 of EP223 are disclosed by Gejdos (see Stirbu 1 ¶242 [**D1/3/279**]).

427. Dr Palerm identified two points of distinction between the disclosure of Gejdos and claim 1 of EP223:

i) First, he said the "*fundamental difference"* is that Gejdos does not disclose a UDPD carrying out installation and functional checks <u>on the safety critical application</u>. The reason for this is that in Dr Palerm's view "*the healthcare management software system described in Gejdos is not an SCA within the meaning of EP 223. … The healthcare management system described in Gejdos is not a 'live' system such as a CGM or drug delivery device but a program for reviewing and storing patient information. … a malfunction of the healthcare management system in Gejdos would not have any significant adverse consequences – certainly not of a kind which would put the health or life of a person at risk"*.

ii) Second, he said "*even if the healthcare management system were considered to be an SCA, no installation or functional checks are carried out on the healthcare management system itself. In contrast … the healthcare management software system carries out an integrity test <u>on the patient database</u>, which is clearly not an SCA but a store of information. Furthermore, the patient data itself is not checked, only other data related to the settings of the units of measurement and the like*".

428. Dr Stirbu did not agree. So these two points were fully explored at trial.

Safety critical application?

429. Dr Palerm had essentially two points as to why Gejdos does not disclose an SCA: first, because it was not a 'live' system and second, because malfunction would not have any significant adverse consequences. Both points were the consequence of him having formed an unreasonably narrow view of the disclosure of Gejdos. For example, in cross-examination he said this:

> What Gejdos describes is, and it is in the context of a blood glucose meter, of patient comes into the clinic for their quarterly check-up. They connect their blood glucose meter to a computer. They download all of the data from the meter into the computer and then the physician can look at retrospective reports of what the glucose measurements were over the past month and then, based on their assessment, be able to make recommendations for the patient of, 'We should change this or that in your treatment', so it is completely a retrospective view.

430. It is quite clear from EP223 that the concept of an SCA is not limited to 'live' systems – see [0027] and [0028] and in particular:

> [0028] In some aspects of the present disclosure, SCA 304 is an application associated with analyte monitoring and/or determination. Example features of SCA 304 may include, for example, one or more of the following: determining analyte amounts or concentrations from a sample (e.g., saliva, blood, other bodily fluid, etc.); receiving measurement data; managing and/or processing measurement data (e.g., logging measurements, providing warnings based on measurement values, providing alternative representations of data in the form of reports, graphs, charts, etc.);

431. In addition, as was demonstrated in cross-examination, it was unclear what Dr Palerm meant by a 'live' system. He was shown Fig 17 of EP223 which shows a mobile phone with an adapter which is used to take a glucose reading from a traditional fingerprick test, which required him to backtrack from his initial view that a live system 'is one that is running constantly, even when the user is not engaged with it, like a CGM', to 'live… is the patient being affected immediately and directly by what is happening'. As Dexcom submitted, there was no basis in EP223 for either of these additional limitations.

432. As to Dr Palerm's second point, as Dexcom pointed out:

i) Gejdos expressly contemplates the possibility that the physiological information will be used by patients and/or healthcare professionals to determine therapy adjustments for the patient – specifically insulin dosages (see [0031] and [0038]).

ii) Gejdos imposes no particular limitation on where, or what kind of device, its healthcare management system will be run: [0025]

> "Computing device 100 may be a general purpose computer or a portable computing device … exemplary devices include desktop computers, laptop computers, personal data assistants ('PDA'), such as BLACKBERRY brand devices, cellular devices, tablet computers, infusion pumps, blood glucose meters, or an integrated device including a glucose measurement engine and a PDA or cell phone."

iii) The latter "integrated device" is precisely what is depicted in Figure 17 of EP223 and described at [0035] – [0041] See also [0041] of Gejdos:

> "Computing device 200 may be used by the patient, a caregiver, or anyone having relevant data pertaining to a patient. Computing device 200 may be located in a patient's home, a healthcare facility, a drugstore, a kiosk, or any other convenient place".

iv) An example was discussed with Dr Palerm of a system which stored information such as a patient's blood type – plainly a safety critical system.

433. Finally, even on Dr Palerm's view that Gejdos would only be used for retrospective review of blood glucose data in the physician's office, it is clear that failure or malfunction of the system could result in harm to the patient caused by misinformed insulin dosage adjustments.

434. In conclusion on this point, it is clear to me that Gejdos discloses a safety critical application.

Installation check

435. In response to Dr Stirbu's evidence on 'installation check', Dr Palerm stated in his second report that "*Gejdos does not describe any checks on the healthcare management system application to ensure that it installs correctly*". As Dexcom submitted, he appears to understand that the installation check of claim 1 of EP223 must involve a check of the software *executable*, and not another component of the software package like a database.

436. However, EP223 is clear that the installation check can involve checking <u>an image</u> of <u>**an** installed safety critical application component</u> – see claim 2. An "installed safety critical application component" can include any file in a software installation package that is loaded onto the UDPD "*<u>in addition to</u> a primary executable file".* Dr Palerm agreed:

> Q. Each of the files that is included in an installation package can be seen as an SCA component; right?
>
> A. Yes, different programmes that make up a larger system.
>
> Q. It could be an image file for the graphical interface of the app, for example?
>
> A. Yes.

> Q. Audio file for an alarm sound?
>
> A. Yes.
>
> Q. Both of those could be directly safety-critical, could they not, if the system is supposed to play an alarm sound, but the audio file for that sound is corrupted and the alarm may not play and the patient may miss it, right?
>
> A. Potentially.
>
> Q. It could include, as one of the components, a database file?
>
> A. Yes.

437. So EP223's installation check is satisfied by checking an image of a single SCA component, including a database file – as Dr Palerm agreed:

> Q. Just imagine for a moment that the component that you are checking is the database of information, and you discover that has not been installed correctly; that would be covered by the method of claim 2, would it not?
>
> A. Yes.

438. Accordingly, Gejdos discloses an installation check as required by claim 1 of EP223.

Functional check

439. Fig 4 of Gejdos suggests that the database integrity check will be triggered for example upon several events other than installation – e.g. "Launch of Healthcare Management Software System", "Change Patient Databases", "Restore Database".

440. Gejdos' database integrity check is ultimately a check on the <u>database</u> of patient information. As such, as I mentioned above, Dexcom accepted that on their primary construction it is not a <u>direct</u> check of whether an SCA *functions properly.* If, as I have held, functional checks can include indirect checks – particularly, the G6 / G7 / D1 Time Check – then Dexcom submitted that there is no obvious reason why Gejdos' database integrity check should not be a functional check. Dexcom compared the two:

    i) if the G6 / G7 / D1 Time Check fails, the ability of the G6 / G7 / D1 Apps to accurately record, store, and display correctly-timed glucose values will potentially have been impaired; and

    ii) if Gejdos' database integrity check fails, the ability of the healthcare management system to accurately record, store, and display patient data (including glucose values) will potentially have been impaired.

441. Another point made by Dr Palerm and put to Dr Stirbu in cross-examination was that Gejdos' disclosure of integrity checks was limited to what it describes as "conversions" which focus on the units used for measurements stored in the database. He explained that his understanding, as a skilled person, was "*that the database integrity information*

will catch any kind of errors that are at the database level". His answer was fully consistent with the express direction at [0043] that "*[t]he integrity test may be any process whereby the accuracy of patient database 104 may be affirmed or denied".* In any event – as I found above, the functional check in EP223 has a very broad scope: if Gejdos' database integrity check is otherwise within that scope there is no reason why a "conversions"-only check – to ensure that the correct units are recorded / displayed – would not satisfy its requirements.

442. Dexcom also drew attention to the fact that Dr Palerm also asserted "*... the single integrity check of the database is not a disclosure of both an installation and a functional check."* The point here seems to be that a functional check cannot also be an installation check. Dexcom agreed – which is why their primary construction requires the functional check to be a direct check of functionality. Dr Palerm's point was not specifically tied to functional or installation checks, and Dexcom submitted that there is certainly good sense in the idea that EP223 has described several different kinds of checks and defined them differently because it thinks they are distinct and serve different purposes. (Dexcom's emphasis).

443. Dexcom developed this point to create a squeeze on Abbott's case on infringement of claims 7 & 9. So, they say, if it is right that a functional check cannot also be an installation check, then why – per Abbott's positive case, in which the G6 / G7 / D1 Time Checks are relied upon for both – should a *functional check* also be capable of being an *environment check*?

444. In my view, the answer to this is as follows. EP223 describes a number of checks, categorising them by purpose. However, I see no reason why the same check cannot fulfil more than one purpose.

Selective enablement

445. Gejdos at [0043] states that an error message may be presented in the event of a failed database integrity check. Dr Stirbu explained that the Skilled Addressee would understand that this includes disabling safety-critical database related functions when the database integrity check fails.

446. Dr Palerm's evidence was that the consequence of a failed check would be that the database file will not be accessible, but that other functionality of the application would remain active.

447. Abbott submitted that if the check relied on by Dexcom is failed, then the database cannot be accessed, but acknowledged that other databases might be able to be accessed. Abbott submitted however that this is nothing like the selective enablement of the non-safety critical features while disabling safety critical features of an application, as required by claim 1.

448. On this point, I accept Dr Stirbu's evidence. Accordingly, Gejdos discloses 'selective enablement' within integers 1.2(c) and (d).

449. For these reasons, I find that Gejdos anticipates claim 1 of EP223.

450. Dexcom also ran an alternative case that if Gejdos did not anticipate, claim 1 was nonetheless obvious over Gejdos. It is somewhat tricky to address this alternative case for two reasons: first, because neither side developed any arguments to this effect; second, because the reason why I have found that Gejdos discloses something within claim 1 is because of the very broad scope of claim 1.

VALIDITY: INVENTIVE STEP

Lebel

451. Lebel is a US patent application published on 7 February 2002, entitled "*Microprocessor controlled ambulatory medical apparatus with hand-held communication device*".

452. Lebel relates generally to ambulatory medical systems that include a microprocessor controlled ambulatory medical device and a separate control device that communicate via telemetry where the medical device has enhanced functionality, Safety features, failure detection, and/or alarming capabilities. Preferred embodiments relate to implantable infusion pumps and external devices for communicating therewith [0002].

453. Lebel discloses a system comprising two components: an implantable medical device ("MD", such as the implantable insulin infusion pump of figure 1) and a handheld communication device ("CD", or "External Subsystem" – depicted in Fig 2 and on the left-hand side of Figure 3), which is described as being configured to operate only with a specific implantable device.

454. The two components are shown schematically in figure 3, reproduced below.

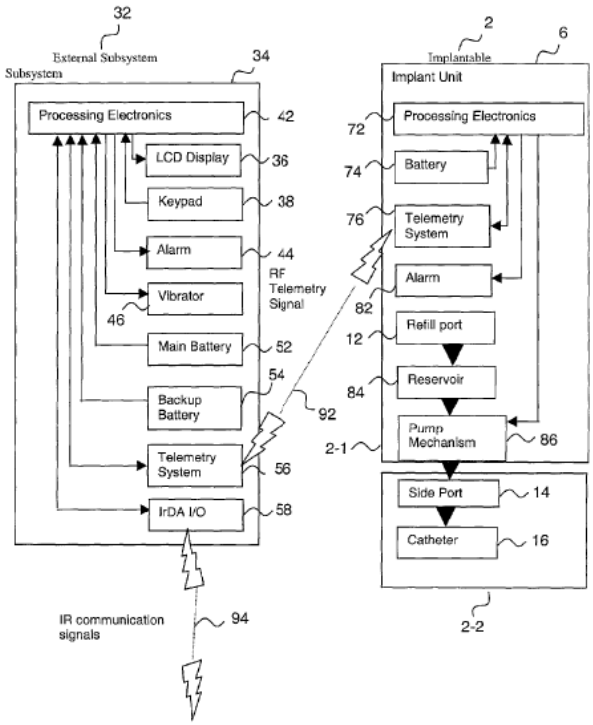


FIGURE 3

455. The implantable device is described as including two processors – a main and a monitor processor. At [0140] Lebel describes a self-checking mechanism whereby the two processors within the implantable device separately perform calculations relating to insulin delivery and the results are compared to ensure the two processors agree on the quantity and timing of insulin delivery. If a problem is identified the implantable device may be placed in "*protective mode*" where insulin delivery is stopped (cut back to a medically insignificant rate).

456. The main processor software can initiate self-test functions, which may be requested via the external communication device or configured to run automatically ([0391]). If the self-test fails, a Watchdog circuit is tripped, which may result in a reset of a processor ([0325]).

457. The implantable device may run both application software and second stage bootloader software ("SSBS"). The bootloader software is described as incapable of operating the insulin pump but capable of performing limited telemetry and communication activity ([0320]). The SSBS can be used to download new application software, remaining in control of the device until the new software is downloaded and executed. It is described as enabling the implantable device to receive new or replacement application software, or allowing the system to reset itself after a system failure, by placing the implantable device in a safe state in which medical functionality (e.g. dispensing insulin) is not supported ([0321]).

Dexcom's case

458. Dr Stirbu considered that the only integer of claim 1 not disclosed in Lebel was integer 1.1 because there was no UDPD. By contrast Lebel disclosed a controlled dedicated medical device. From that starting point there were three main parts to Dr Stirbu's evidence to the effect that an obvious development of Lebel was to replace the control device in Fig 3 with a mobile phone:

i) The first was that the Skilled Team would understand Lebel to provide a range of broadly applicable risk mitigation strategies, which could be used in the context of a range of medical devices. In that regard, Dr Stirbu explained that the skilled person would be familiar with requirements to mitigate risks associated with any medical software, including that installed on a UDPD. In particular, he had mentioned that there are a range of UDPDs, and he believed that the types of devices considered in paragraph 176(a) (e.g. desktop PCs built by the user) would have been on the skilled person's mind because there is no real practical hurdle in applying the techniques of Lebel to a device like that.

ii) The second was that there was a real drive to have medical devices connected to mobile devices at the time and therefore Dr Stirbu believed that the skilled person would have thought about applying the method of Lebel to a mobile phone too. As a result, it would be obvious for the skilled person to take the risk mitigation methods disclosed by Lebel and apply them to any safety critical application, including one which would be installed on a UDPD such as a desktop PC, laptop or a mobile phone.

iii) On the third plank, Dr Stirbu reasoned as follows:

> 'If you consider the Lebel system, the control device shown in Figure 3 includes many of the features of a mobile phone such as an LCD, the input keys, the alarm, the vibrator, and the battery, so it would be obvious for a skilled person developing an improved device starting from Lebel, to replace this part of the device with a mobile phone.'

459. It is fair to acknowledge that Dr Stirbu explained (in both his reports) that there was a spectrum of devices which fall within the definition of a UDPD which allow a user varying amounts of freedom to make hardware and software changes. He pointed out that Apple iOS and Android operating systems strictly controlled what applications could be installed on a phone (due to the App Store verifications process he had described earlier) and the process of installation. He also pointed out that the types of checks characterised in EP223 as 'installation checks' and 'functional checks' were checks which were (and known to be) checks typically carried out by the operating systems and/or other programs on smartphones, such that many of them would be known by the Skilled Team to be redundant in the context of a smartphone.

Dr Palerm's evidence

460. As I mentioned above, Dr Palerm accepted that the idea of hosting an SCA on a UDPD was not part of the inventive concept of claim 1 of EP223. As such, Dexcom submitted that it is legitimate to approach each item of prior art on the basis that the skilled addressee has been tasked with implementing (say) CGM functionality in a smartphone app. I agree that there is no hindsight in posing the obviousness question in this way: see the judgment of Birss J (as he then was) in *HTC Corp v Gemalto SA* [2013] EWHC 1876 Pat at [267] – [276].

461. In his written evidence, although he considered the inventive concept of claim 1 of EP223 to be relevant to a person who has already had the idea of hosting an SCA (such as a CGM reader) on a UDPD and is thinking about how to make it happen safely,[2] Dr Palerm approached Lebel entirely in the abstract, asking himself about what the Skilled Addressee might do if the document was placed on their desk *apropos* of nothing:

> 18 Q. You have approached Lebel on the basis that the skilled addressee is not interested in putting a SCA on an UDPD when they read it and then asked if that would prompt them to do so; right?
>
> A. Correct. The SCA in this case, this is one, even the hand-held device, you could not even put that on an uncontrolled mobile phone today, because the frequencies that it uses to communicate with implantable pump require a special radio set that a mobile phone does not have. ….

462. Thus, Dr Palerm's primary and "fundamental" objection to the alleged obviousness of EP223 in light of Lebel – that it "does not concern an SCA installed on an uncontrolled data processing device of any kind" and "it would not … have been obvious to the EP223 Skilled Team to install such SCAs on UDPDs, nor specifically mobile phones,

[2] [**T/2/297$_{22}$ – 298$_{2}$**]

and there is nothing in Lebel to suggest doing that, nor [that] any aspect of the functionality that it describes might be useful in such a context. …" (Palerm 1 ¶¶19.4 – 19.5) – was misguided. Dr Palerm was looking for an express direction in the prior art to deploy its teaching in the context of SCAs hosted on UDPDs, but he did not need to look for one there since the idea was itself part of the CGK.

Abbott's criticisms

463. Abbott focussed on the suggestion that the Skilled Team would seek to implement the reader device (figure 2 and the left-hand side of figure 3) in a smartphone app, but (as Dr Stirbu acknowledged) they would not seek to take the software in the implantable infusion pump off the device and put it on an app.

464. Abbott contended that this case suffered from such insuperable problems that it could only have been constructed by Dexcom/Dr Stirbu working backwards from the invention. Abbott made the following points:

i) First, there is no suggestion of implementing the reader in a smartphone app in Lebel; and (unless the skilled person is defined in a way that means they have to create a smartphone app), that is the end of Dexcom's case.

ii) Second, even if the skilled person were to consider creating such an app, Lebel does not teach anything that would help the skilled person in that situation. The ecosystems are so different (dedicated device & software created together vs. an app written for a third-party device and OS) that it would require a large amount of imagination to seek to adapt the strategies used in Lebel to that different ecosystem.

iii) Third, in relation to the installation check, Dr Stirbu referred to the teaching of Lebel at [0320] and [0391]. But that teaching relates to installation of software on the implantable pump, not the reader which Dr Stirbu's skilled person is supposedly replicating on an app. It would be a significant leap to seek to implement those ideas in the completely different context of the reader.

iv) Fourth, it is a very different type of installation. The disclosure relied on by Dr Stirbu relates to fresh installation of the application software each time the implanted pump is turned on. That is a wholly different context to downloading and installing an app from an app store.

v) Fifth, the functionality relied on in relation to the installation check is carried out by "bootloader" software, which is firmware (i.e. not application layer software). In a UDPD context, its functionality would be carried out by the OS and would not be a matter for the app developer at all – indeed, the app would be prevented from doing any such functionality.

vi) Sixth, in relation to the functional check, Dr Stirbu referred to the teaching of Lebel at [0140] – [0147]. But that teaching also relates to the implantable pump, not the dedicated reader which Dr Stirbu's skilled person is supposedly replicating on an app. Again, it would be a huge leap to seek to implement those ideas in the completely different context of the dedicated reader.

vii) Seventh, the functionality relied on in relation to the functional check is carried out by (i) "bootloader" software, as to which see v) above and (ii) watchdog circuits, which comprises "control electronics" such as described at [0140]. Obviously nothing like that can be implemented in application software in a UDPD.

viii) Eighth, the functionality relied on in relation to selective enablement is the same teaching which relates to the implantable pump, not the dedicated reader which Dr Stirbu's skilled person is supposedly replicating on an app. The same points apply again.

ix) Unsurprisingly, Dr Stirbu eventually agreed that a skilled person reading the disclosure of Lebel relied on would think "Well, I cannot do anything like this, because I am writing application software".

465. The technical points in that list were established by Abbott in their cross-examination of Dr Stirbu. As for point ix), Dr Stirbu did agree that point, but it was clear he was genuinely puzzled about the distinction being drawn by the cross-examiner between application software and firmware. I think this resulted from Abbott's contention that the Skilled Person was a writer of application software and not firmware.

466. As Dexcom pointed out, Abbott's list of points includes some repetition. Furthermore, they also include some misdirection and fail to address the actual case which Dexcom put forward.

Analysis

467. A point made by Abbott in their Opening was that neither Dr Stirbu nor Dexcom had spelt out precisely how, in their obviousness case, the Skilled Team got from Lebel to something which fell within claim 1.

468. It became clear to me from Dr Stirbu's evidence that he was envisaging a route at quite a high level of generality. The Skilled Team was presented in Lebel with a range of broadly applicable risk mitigation strategies, and I think his point was that the Skilled Team could select from that range those which suited their purpose. In contrast, his cross-examination entirely legitimately delved into the detail and did not engage at any higher level.

469. However, inherent in Dr Stirbu's approach was his acknowledgement that the installation checks and functional checks in, for example, an iOS environment were already supplied by the operating system (see paragraph 459 above). He may have thought therefore that all that was required was to replace the dedicated reader with a UDPD in the shape of a smartphone. As he readily accepted in cross-examination, his Skilled Team were not moving any software from the implantable pump to the UDPD. However, I think his point was that the dedicated reader in Lebel had to contain software to analyse and display results sent to it from the implantable pump e.g. blood glucose levels, and that software would be placed on the UDPD, and it would undergo the standard iOS or Android 'installation checks' and 'functional checks' within the meaning of those broad expressions in claim 1 of EP223.

470. If this case had been spelled out, one final obstacle to it is the fact that it does not require the application of any of the risk mitigation strategies taught in Lebel. Instead, the Skilled Team would have to realise that the addition of any of those strategies was not needed.

471. Overall, I am unable to accept that EP223 was obvious over Lebel for two principal reasons. First, because the route taken in the obviousness attack was not spelled out (either at all or clearly enough). Second, because the attack seemed to me to be essentially an argument that it was obvious (from the CGK) to replace the dedicated reader unit in Lebel with a UDPD.

472. It is convenient at this point to address Dexcom's Gillette arguments.

Dexcom's Gillette arguments

473. Dexcom's Gillette argument is constructed from a number of discrete points, as follows.

474. First, the Signature Check relied upon by Abbott as satisfying the requirement of claim 1 to "determin[e] whether the SCA is installed properly" was inevitably carried out at the priority date of EP223 whenever any iOS or Android app – of any kind – was installed through the respective App Store (and, indeed Dr Palerm said that installation checks were "pretty much" known "from the beginning of software onwards". Dr Palerm also agreed :

> Q. Indeed, every single app available on the iOS or Android App Stores, whether it is Dexcom G6 app or Angry Birds, it undergoes the same signature verification process?
>
> A. Yes.
>
> Q. It is the same one that has been used in iOS and Android since before September 2009; right?
>
> A. Yes and if not exactly the same, something very similar.

475. Second, partial disablement. On this, Dr Palerm made clear that the partial disablement aspect of claim 1 of EP223 was (i) a matter of user experience rather than safety; and (ii) obvious in the event of the detection of an app failure or malfunction as an alternative to total disablement – e.g. the SCA itself may retain the functionality necessary to display a message "cannot run right now" in the event a problem is detected:

> Q. Sure, but what you are saying in [¶17.23(b) of Palerm 1] is about them being allowed to continue to access non-safety-critical aspects. That is about the user experience.
> A. Yes.
> Q. Not about the safety.
> A. Correct.
> Q. You could keep the user safe from harm caused by a software malfunction simply by disabling the SCA altogether when a check failed, yes?
> A. That is a possibility.
> Q. But that would be a worse user experience, less convenient, et

> cetera?
> A. Correct.
> Q. If you totally disable the app so it will not run at all, the user will find that a bit puzzling. They will not know why the app is not opening?
> A. I would expect at that point some sort of message would be given to them or an error message of some sort notifying why it will not run.
> Q. Not from the app, because the app is not running.
> A. It could be from the app itself, that you run the app and you simply have a message, "Cannot run right now".

476. The result is, so Dexcom submitted, that the only issue on obviousness, on Abbott's construction, is whether it would be obvious to include within a SCA smartphone app (such as a CGM reader app) on a smartphone a functional check of some kind (which can include checking whether the system time is accurate). This is the third point.

477. When addressing this third point – the obviousness of implementing a functional check – Dexcom submitted that the language of claim 1 places no express limitation at all on the functional check required: just "determining ... whether a safety critical application … functions properly". Accordingly, they submitted it seemed to be common ground that:

i) only one aspect of the SCA's functionality needs to be checked to satisfy the claim (noting that Abbott's infringement case relies solely upon the Time Check);

ii) there is no requirement that the check has any particular level of sensitivity or specificity for detection of problems;

iii) the check on the SCA's functionality can be carried out by the SCA itself (see Abbott's infringement case on the Time Check), by the operating system (see Abbott's infringement case on the Signature Check), or by a separate piece of software (the "test harness" of EP223).

478. Accordingly, Dexcom submitted that in this respect the claim is exceptionally broad – any kind of functional check on a single aspect of the SCA's functionality carried out by any software component will do (although on Dexcom's construction the check needs to directly check the functionality concerned while Abbott says that an indirect check (e.g. checking the system clock) is sufficient).

479. Finally, Dexcom submitted that this analysis also applied to claims 7&9, since Dr Palerm agreed that checks on the time would be obvious when seeking to implement a CGK reader in a smartphone app.

480. For the moment, I leave claims 7 & 9 until later. As for the three discrete points pertaining to claim 1, I accept that Dexcom established all three points on an individual basis. However, the problem lies in identifying the starting point for the obviousness argument which utilises these three points. It seems to me there are only five possible options: i) Gejdos, ii) Lebel, iii) an unpleaded case of obviousness over CGK, iv) a contention (which was not made) that no starting point is required because it is a Gillette

argument or v) an argument of lack of technical contribution/AgrEvo obviousness. Dealing with each in turn:

i) First, no-one explained how these three discrete points can be applied in the rather different context of Gejdos.

ii) Second, as for Lebel, again there was no attempt to combine any of these three discrete points into the obviousness argument over Lebel.

iii) Third, it seems to me that Dexcom's three discrete points most obviously lend themselves to an argument that claim 1 of EP223 was obvious over the CGK. It is well known that an argument that a claim is obvious over the CGK must be pleaded and, if pleaded, it is now frequently the case that the party alleging invalidity on this basis is required to serve a statement of case identifying the specific CGK relied upon. Yet further, the warnings about cases of obviousness over CGK are also well known: see Floyd J. in *ratiopharm v Napp* [2008] EWHC 3070 (Pat), [2009] RPC 11 at [155]-[159], and Birss J. in *Accord v medac* [2016] EWHC 24 (Pat) at [120]-[124]. However powerful I might have considered the argument to be, if it had been pleaded, it has not been pleaded with the result that Abbott have had no occasion to address it. In these circumstances, I am unable to deal with this unpleaded allegation.

iv) Fourth, 'Gillette' is not a magic wand. As Terrell says (19th Edition at 14-313 '*It [the Gillette defence] is in reality an attack on validity which invokes the policy underlying the grounds of anticipation and obviousness*.' It remains necessary to establish the underlying ground, in this case, of obviousness.

v) That leaves the argument of lack of technical contribution. This was pleaded, albeit that Abbott referred in closing to the 'unparticularised plea of lack of technical contribution'.

481. However, the reason why I thought it right to consider these five options is because Dexcom did not address lack of technical contribution directly in either their written or oral closings. Abbott did address it in their written closing, contending that they did not understand how such a plea could be sustained. That, of course, was a clear invitation to Dexcom to spell out how it could be sustained. Since that did not happen I decline to spend any more time on it. It would have been more helpful if the Gillette argument had either been explained properly or been dropped.

Claims 7 and 9

482. In his evidence, Dr Palerm dealt with the inventive concept of claims 7 and 9 together, a point which Abbott adopted in their written closing. In other words, there was no attempt to suggest that claim 7 was independently inventive. So I will deal with these two claims together.

483. Dexcom's closing addressed these two claims on the alternative constructions:

i) **On Abbott's apparent construction**: Dexcom submitted that claim 9 is blindingly obvious – just repeat any functional check, and the claim will be satisfied. It cannot seriously be suggested that if it is obvious to do a functional

check, it is not obvious to repeat it. Lebel's watchdog circuits, for example, monitor for errors on a continual basis. As Dr Palerm put it [**T/3/361$_{6-14}$**]:

> In the case of time, if you will, the check of a change of environment is more trivial because by its nature, time is advancing. There are other environment checks that require additional, like a change: 'Has the operating system changed? Has a new version of the operating system been installed on the device?' And the like, but time is passing, so there is an implicit check there that time is moving on

ii) **On Dexcom's construction**: Dr Stirbu was not challenged by Dr Palerm or in cross-examination on any of his evidence (on infringement or validity) on claims 7 / 9 of EP223. He explained that the concept of an environment check was well-known and did not see any inventiveness in the way it was deployed in EP223.

484. Dexcom also submitted that Dr Palerm's own evidence confirmed that there was nothing inventive about performing a check of the hardware or software environment (see [**T/3/365$_{11}$ – 367$_{12}$**]):

> Q. The skilled person who is interested in hosting an SCA on an UDPD knows that the system environment is not controlled; yes?
>
> A. Correct.
>
> Q. They would foresee that some kind of system environment might change; yes?
>
> A. Yes.
>
> Q. I think that is what you said was your immediate concern in 2009?
>
> A. Correct.
>
> Q. They would be worried that the software might install and run perfectly well for a time but cease to do so if the user made a change to the environment on the UDPD; yes?
>
> A. Correct.
>
> Q. Changed the hardware, upgraded to a new version of iOS or something like that; yes?
>
> A. Correct.
>
> Q. The skilled person would know that they needed some kind of environment check, but with a SCA, they would be worried about whether that would be robust enough; yes?

> A. Yes, and it is more than just – The environment check is definitely an important piece of this. It is the functional checks that you perform after that are the more important part, because one of the most common pieces of it would be: I perform an environment check; I have done all of my testing in the engineering bench top, if you will; and I know that it works; and I will just make numbers up, iOS 6, and the user has just upgraded to iOS 7; me, the manufacturer, I have not performed the testing on iOS 7, so I am going to prevent the application of running at all if they happen to upgrade to iOS 7 before I am able to whitelist that operating system as an acceptable environment to operate in. In this case the functional checks are about how do I still allow a certain level of functionality, even in the face of such changes? What type of functional checks can I perform on the device to prevent all of this, all or nothing type of response.
>
> Q. They would anticipate they would need some environment check.
>
> A. Yes.
>
> Q. And they anticipate that they would need to have some consequence if the environment had changed; yes?
>
> A. Yes.
>
> Q. And then you are saying the devil would be in the details as to what they did afterwards; yes?
>
> A. "Devil in the details" in what sense?
>
> Q. I am using an idiom. They would have to decide how they responded to a detection that the environment had changed; yes?
>
> A. Correct, and the standard approach had been environment change, it has changed in a way that I have not been able to test, like the change in operating system and completely preventing the application from operating from that point.

485. Elsewhere in his cross-examination, Dr Palerm refused to accept that running an environment check was obvious, falling back on generalised safety concerns. This was not convincing at all. In the circumstances I find claims 7 /9 obvious over claim 1.

EP159 & EP539

Introduction

486. EP159 is entitled "*Systems and Methods for Providing Sensitive and Specific Alarms*" and EP539 is entitled "*Systems for Providing Sensitive and Specific Alarms*". They share the same priority date (unchallenged) of 30 October 2012. They are related (EP539 is a divisional of EP159). The specifications of the two patents are virtually identical though there are some differences in paragraph numbering. I propose to refer to paragraph numbers of EP539.

487. Only one claim of each patent is in issue – claim 1 of EP159 and the unconditionally proposed amended claim 1 of EP539. Abbott admits infringement of both claims.

488. As Abbott submitted, the inventive concept of the claims of the Dexcom patents (which is effectively the same for EP159 and EP539 as proposed to be amended) is the provision of (at least) two hypoglycaemic alarms, one a current glucose alarm with a user settable threshold and the second a predictive alarm with a fixed threshold.

489. Abbott's case is that combination of alarms was no more than one common-sense way to implement glucose alarms of a kind that were well known to the skilled team from the products on the market. For that reason, there was much focus on the CGK as to the available products on the market which the skilled person would be aware of and what the skilled team would have learned from them. Armed with the CGK, Abbott submit both claims were anticipated by Brauker 2007 and Shariati but if not anticipated obvious over those and two other citations, the STS-7 Guide and the Navigator Guide.

490. Dexcom's case is that the claims were neither anticipated nor obvious, making the familiar accusation that Abbott's case was infused with hindsight. Furthermore, it was plain from Professor Oliver's evidence that Dexcom appeared to be running a mindset case against both fixed and predictive alerts. This was addressed in some detail in Abbott's written opening, but hardly touched upon in Dexcom's, the only references to mindset coming in some general citation of authority on the skilled team (*Schlumberger* [42] and *Teva v Leo* [2015] EWCA Civ 799 at [29]).

491. However, the mindset case seemed to be the cause or driver for disputes as to (a) the Skilled Addressee/Team of the Patents and (b) their CGK.

492. The status of the mindset evidence became more obscure when in their Closing Dexcom disclaimed any reliance on a mindset case. This was put at the very start of their written closing:

> '1. The central dispute in this case is obviousness. The inventions claimed in EP159/539 are relatively simple, and straightforward to implement once they have been described. There are two possible reasons why an invention of this nature will not obvious:
>
> (a) the invention is one which the unimaginative Skilled Addressee just would not arrive at, having read the prior art; or
>
> (b) the invention is one which the unimaginative Skilled Addressee would arrive at – but would then reject for reasons of technical prejudice.

> 2. Dexcom's answer to the obviousness attacks in this case is – as we made clear in opening – the first kind set out above: the unimaginative skilled team reading Shariati, Brauker 2007, the Navigator Guide, or the STS-7 Guide in October 2012 simply would not have arrived at a CGM system with a user-settable current hypoglycaemia alarm and a fixed-threshold predictive hypoglycaemia alarm. Dexcom does not have a fallback position relying upon the second kind of non-obviousness argument.'

493. On reflection, it is perhaps not surprising that Dexcom disclaimed the second kind of non-obviousness argument because, if there was a technical prejudice, these Patents neither discuss it nor explain why it was unwarranted. Hence Dexcom had to argue that the invention simply would not occur to the Skilled Team, having read and considered each piece of prior art. So the focus switched from mindset to the *context* within which the Skilled Team would read each piece of prior art, which was also the backdrop for Dexcom's accusations of hindsight. On context, Professor Oliver's evidence remained relevant although I am bound to say that, on the facts here, the distinction between the two cases seemed to be very thin indeed.

494. For these Patents, it is convenient to deal with the identity of the Skilled Addressee and their CGK first, then to discuss the Patents and their claims. Since the EP539 claims are those in the proposed unconditional amendment, it is convenient to consider the objections to the proposed amendments before moving to the main validity attacks.

The EP159 / 539 Skilled Addressee

495. It is common ground that the Skilled Addressee is the same for EP159 and EP539.

496. Dr Palerm said that EP159 and EP539 are addressed to a team lead by an engineer who would consult with:

i) a systems engineering team;

ii) a human factors team (individuals concerned with developing effective interfacing between a human user and the device); and

iii) a clinical education team, which would include individuals who may or may not be clinicians, but who would have specific knowledge of diabetes and its management.

497. Prof Oliver took the view that EP159 and EP539 are addressed to a Skilled Clinician; but he says that to the extent that the addressee is a Skilled Engineer, it is a Skilled Engineer who works very closely with, and seeks advice from, a Skilled Clinician.

498. Each expert disagreed with the other in this regard:

i) Prof Oliver considered, essentially, that Dr Palerm's focus on the engineer was wrong: when deciding on how to implement hypo and hyperglycaemia alarms for a CGM, the clinician's expertise and experience is an essential input into the process of designing CGM alarms.

ii) Dr Palerm takes the view that Prof Oliver has overstated the role of the clinician in the CGM design process. He says that while clinicians "might be consulted

by the design team about specific issues at specific stages of the process", a major role for clinicians is in developing clinical trials for a new product. He seemed to take the view that an engineer working in the field of diabetes would have sufficient knowledge to understand the "medical aspects" of EP159 / 539.

499. I agree with Dr Palerm on this point in that an engineer working in this field would have sufficient knowledge of, in particular, the various clinical guidelines. It seemed to me that Professor Oliver's insistence on a much greater role for the clinician was simply a foundation for his argument that the academic discussion and debate over trying to define an accepted glucose level to be used as a yardstick for use in clinical research studies concerning hypoglycaemia, so that research studies could be compared, was part of the CGK. It was not.

CGK points in dispute

500. The agreed CGK is set out above. Here I deal with the CGK points in dispute on these Patents.

501. At the start of the trial I was presented with lists of CGK points in dispute – lists because the parties could not even agree what was in dispute. In relation to these Patents, Abbott suggested that the following matters were in dispute:

i) whether the Dexcom G4 (2012) and its features were CGK. I could not see how this made the slightest difference so I do not consider it further.

ii) The significance, if any, of the following on CGM device design in 2012:

a) The level of consensus on the appropriate blood glucose values for defining hypoglycaemia.

b) Glycaemic variability.

c) Alarm fatigue.

d) The accuracy of CGM devices.

502. Although each of those issues featured (in one form or another) in Dexcom's list of disputed CGK issues, Dexcom listed another 14 issues. Although I have reviewed this list again for the purposes of preparing this judgment, they do not seem to me to be material. It is sufficient to focus on the four issues identified by Abbott.

Level of consensus on blood glucose levels for hypoglycaemia

503. I have already touched on this. The academic debate over a definition for adoption in clinical research trials was not part of the CGK.

504. To the contrary, as Dr Palerm explained, there were two commonly accepted or recognised thresholds. First, it was commonly accepted that 70mg/dL (3.9mmol/L) was a threshold for biochemical hypoglycaemia. Second, it was commonly recognised that symptoms of cognitive impairment may be seen in most patients at or below about 50-54mg/dL (2.8-3.0 mmol/L) and this would be regarded as a potentially dangerous

level of hypoglycaemia, and one, in Dr Palerm's view, the CGM designer would have wanted to alert the patient.

505. These thresholds were consistent with the practical clinical guidance from (a) the 2005 American Diabetes Association Report, (b) the 2011 Oxford Textbook of Endocrinology and Diabetes, (c) the May 2012 EMA Guideline which describes the ADA classifications as a 'well-accepted source', as well as (d) the 2009 Position Statement from the ADA. These thresholds were also consistent with those used in actual devices.

Glycaemic variability

506. Professor Oliver's point was that glycaemic variability experienced between individual users would lead the Skilled Team to not include a fixed alarm in a CGM. Dr Palerm disagreed. He was of the view that the Skilled Team would consider the overall alarm system rather than each alarm in isolation and would understand that including a user-settable alarm would enable an alarm to be set according to a user's preference. However, Dr Palerm considered it would remain attractive for the Skilled Team to include a fixed alarm at a clinically significant level (such as 3.0 mmol/L) to provide a safety net (cf the fixed alarm in the STS-7).

507. Whilst glycaemic variability was well-known, I agree with Dr Palerm on this point.

Alarm fatigue

508. Alarm fatigue was a known issue, but Dr Palerm was of the view that it originated mainly from alarms for which corrective action was not needed (e.g. an alarm at 5.0 mmol/L). What he described as the 'trade-off' in a user-settable alarm between a lower threshold which would catch fewer actual instances of hypoglycaemia and an artificially high threshold which would risk alarm fatigue, would not have been a significant factor in the Skilled Team's decision to include a fixed predictive alarm threshold.

509. Dr Palerm also made the point that the trend in CGM device design was to include more alarms rather than fewer. Alarm fatigue was not a concern because most alarms could be disabled. Understandably however, a low fixed alarm (such as 3.0 mmol/L) could not be disabled because it was safety critical. I agree with Dr Palerm on this point.

The accuracy of CGM devices

510. The experts were agreed that improving CGM device accuracy was a constant development objective of CGM manufacturers. Professor Oliver seemed to suggest this objective would so dominate the thinking in the Skilled Team (the Skilled Clinician in particular) that they would not arrive at the claimed invention of these Patents. Dr Palerm did not agree that improving accuracy would exclude development of other CGM features, such as alarms. Dr Palerm also made the point that the accuracy of the signal processing algorithms would be for the signal processing engineer, and the accuracy of the device a matter for the sensor design team. Thus, sensor accuracy would be a design parameter presented to the Skilled Team of these Patents.

511. Furthermore, all the CGM devices were adjunctive, providing warnings to be confirmed by fingerprick testing. Dr Palerm was of the view that potential inaccuracies in the CGM glucose measurements provided a positive reason to include a 'safety net' alarm (e.g. at 3.0mmol/L), and particularly a predictive alarm at that level to give the user advance notice. Once again, I accept Dr Palerm's evidence on this point.

The Specification(s)

512. The descriptions cover many aspects of the functionality of a CGM device and there are other patents deriving from EP159. The claims in these two have picked out certain features and put them together in a particular combination. I have picked out the paragraphs most relevant to the claims. In summary:

i) The patents set out to allow users to receive alerts or alarms indicative of glycaemic condition in a "*more accurate and useful way*" ([0010] – under Summary).

ii) The patents describe various components of a continuous analyte monitoring system from [0023] – [0074]. This includes visual displays showing glucose information in the form of a trend graph and a single numerical value ([0058] and figure 4A). The trend graph shows upper and lower boundaries representing a target range in which the user should maintain their glucose. The visual boundaries shown may be different from the boundaries that generate an alert ([0071]).

iii) A low alert screen is displayed when the user's glucose drops below a "*pre-set limit*", shown as 55mg/dL ([0059] and figure 4B. Dr Palerm pointed out this replicates the "Low Glucose Alarm" screen in the STS-7. A "*Going Low*" alert is also described to indicate to the user that their blood glucose will soon be in the low range ([0063] and figure 4D).

iv) Predictive alerts may be provided when a severe hypoglycaemic event is predicted to occur in the near future, the example given being a blood glucose value of 55mg/dL. In such a case the processor is said to be programmed with a blood glucose value below which the user is considered to be hypoglycaemic ([0064] – [0065]).

v) At [0075] – [0123], the patents describe predictive alerts. The rationale for such alerts is said to be that it is desirable to prevent hypoglycaemia and/or hyperglycaemia episodes instead of simply generating alerts when episodes occur ([0076]). Abbott correctly submitted that the skilled team would be familiar with this concept, since several CGK CGM devices used predictive alerts and the value of such alerts was well understood, e.g., a patient with a warning of a likely hypoglycaemic event could ingest carbohydrate and prevent the threatened episode entirely.

vi) Paragraph [0075] also describes applying a conversion function to the signal received from the sensor which may take into account variables such as temperature. The parties agreed that such functionality would have been standard practice for a CGM design team.

vii) Figure 5 (introduced in [0077] and shown below) shows a system with three alert thresholds: TV_1 and TV_2 are user-settable thresholds for high and low glucose alerts, respectively. TV_P is "*the predictive threshold e.g., the threshold against which a predicted value is compared*"

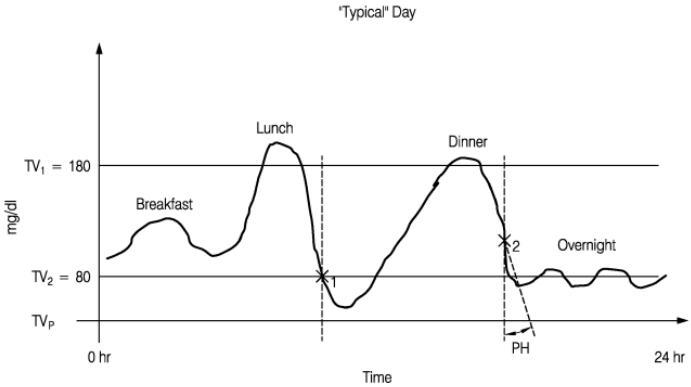


FIG. 5

viii) The full context is in [0078] which I set out because it features in one of the arguments I have to consider later:

> '[0078] As shown, there are three threshold values or limits used in the monitoring of the glucose values in some embodiments: TV_1, TV_2 and TV_p. TV_1 is settable by the user and generally defines the upper limit or upper glucose value that a user may operate at before being alerted by the monitor. Similarly, TV_2 generally defines the lower limit or lower glucose value that a user may operate at before being alerted by the monitor. TV_p is the predictive threshold, e.g., the threshold against which a predicted value is compared. It should be appreciated that although the illustrated embodiment envisions a threshold value, threshold ranges or other criteria (e.g., glycemic states) may alternatively be used.'

ix) [0079] explains that 'TV_P may not be settable by the user; it may be a fixed value or permanent value set during factory settings'. TV_p may be a fixed value representing a dangerously low glucose value e.g. a value indicative of a serious hypoglycaemic event. The example given is a value at or around 55mg/dL. Paragraph [107] further states that it is desirable to have a threshold that cannot be changed by the user due to the importance of the threshold, and repeats the example of a value of 55mg/dL indicating a severe hypoglycaemic event. Abbott point out that there is no explanation of why that value is chosen or mention of any uncertainty surrounding that value as an appropriate threshold.

x) Flags X_1 and X_2 are described at [0081] – [0082]. X_1 is described as a threshold flag which alerts the user if a first threshold (e.g. TV_2) has been met. X_2 is a "predictive flag" which alerts the user that threshold TV_P is predicted to be met within a predefined time frame.

xi) [0085] – [0086] describe a "target zone" which may be shown on the display (shown in figure 3B). [0087] states that the visual target zones may be different from the thresholds for TV_1 and TV_2 (said to define the alert boundary) which may not be displayed to the user.

xii) A process for providing a predictive alert is shown schematically in figure 6. Examples of algorithms for generating a predictive alert are described at a high level at [0101] – [0104]. Although the algorithms differ, it is clear from those paragraphs and subsequent ones that a predictive alert is based (not surprisingly) on a range of glucose values over time and not on a single current value.

CONSTRUCTION - claim 1 of EP159

513. Claim 1 of EP159 was broken down into integers as follows:

1	a	A system (100) for processing data, the system comprising:
	b	a continuous analyte sensor (8) configured to be implanted within a body; and
	c	sensor electronics (12) configured to receive and process sensor data output by the sensor, the sensor electronics coupled to a processor module,
		the processor module configured to:
	d	apply a conversion function to sensor data, the conversion function taking into account temperature correction;
	e	evaluate sensor data (520) using a first function to determine whether a real time glucose value meets one or more first criteria, wherein the one or more first criteria comprises a first threshold that is configured to be settable;
	f	evaluate sensor data (530) using a second function to determine whether a real time glucose value meets one or more second criteria, wherein the one or more first criteria comprises a second threshold that is a fixed value;
	g	activate a hypoglycaemic indicator (540) if either the one or more first criteria or the one or more second criteria are met; and
	h	provide an output (550) based on the activated hypoglycaemic indicator.

514. Although Dexcom's Opening Skeleton included a detailed analysis of each integer, there seemed to be no dispute about the interpretation of the claim. Stripped of the verbiage, what is claimed is the provision of two types of hypoglycaemic indicators based on two thresholds, where the first threshold is configured to be settable and the second threshold is a fixed value.

515. Abbott submitted:

i) That the specification makes it clear that 'settable' means settable by the user or some person on their behalf, in contrast to the fixed predetermined threshold which cannot be altered. Dexcom agreed.

ii) That 'the fixed value' in integer 1(f) means a predetermined threshold which is not settable i.e. one which the user cannot change. Again, there seemed to be no dispute about this.

516. Accordingly, EP159 claim 1 can be summarised as claiming a system with a continuous analyte sensor including:

i) a user-settable current alert (integer 1(d) together with (g) and (h)),

ii) a fixed predictive alert (integer 1(e) together with (g) and (h)),

iii) a temperature conversion function (integer 1(d)).

CONSTRUCTION – claim 1 of EP539

517. Claim 1 of EP539 as proposed to be amended is long, but it is worth setting out to show where integer 1(f), as proposed to be amended and which is the subject of controversy, sits in relation to 1(e), (g) and (i). The proposed amendments are shown in italics and underlined, for clarity:

1	a	A system (100) for processing data, the system comprising:
	b	a continuous analyte sensor (8) configured to be implanted within a body
	c	sensor electronics (12) configured to receive and process sensor data output by the sensor (8); and
	d	the sensor electronics (12) coupled to a processor module (214), the processor module (214) configured to:
	e	evaluate sensor data to determine whether a real time glucose value meets a first threshold *(TV$_2$)* that is configured to be settable;
	f	evaluate sensor data to determine whether the real time glucose value meets a second threshold *(TV$_p$) in a predetermined time frame or time horizon*;
	g	activate a hypoglycaemic indicator if either the first threshold *(TV$_2$)* or the second threshold *(TV$_p$)* are met; and
	h	*provide an output based on the activated hypoglycaemic indicator, wherein the output comprises at least one of an audible, tactile or visual output, and wherein the output is differentiated and/or provides information selectively based on whether the hypoglycaemic indicator was activated based on the first threshold or whether the hypoglycaemic indicator was activated based on the second threshold;*
		characterised in that
	i	the second threshold is a fixed predetermined threshold, *wherein the second threshold is not settable*,
	j	*wherein the processor module is configured to visually display a glucose target range with a high target boundary and a low target boundary on a user interface, and wherein the low target boundary visually displayed is different from the first threshold*
	k	*and wherein the high target boundary visually displayed is different from a third threshold (TV1) associated with a hyperglycaemic*

		indicator, such that the range between the first and third thresholds is wider than the range between the low and high target boundaries.

518. The only issues of construction relate to the amendments to EP539 and I deal with them in the next section.

EP539 Amendment

519. Abbott maintained two objections against the proposed amendment of EP539. The amendments are said to extend protection and to lack clarity and precision.

Extension of protection

520. Dexcom drew my attention to the following passage from the judgment of Birss J in *Hospira v Genentech* [2014] EWHC 3857, where he addressed this objection:

> "106. This rarely comes up at trial in the UK, no doubt because the law is clear and usually easy to apply. The correct approach is to compare the scope of the claims as granted with the scope of the claims as proposed to be amended. In both cases the scope is that of the claims properly construed in accordance with the Protocol. If the proposed amended claim covers something that would not have been covered by the granted claims then the prohibition is engaged.
>
> 107. Usually to make the argument good the person challenging the amendment needs to identify a concrete thing which did not fall within the scope as granted but which would fall within the scope after amendment if the amendment was allowed. If such a thing cannot be identified in concrete terms, that is usually an indication that there is no extension. Because the prohibition is absolute, the thing need not be commercially realistic."

521. The allegation here concerns integer 1(f). However, Abbott contended the amendment needed to be considered against the backdrop of integers 1(e), (f) and (g), to which I add 1(i) and the fact that 1(f) sits in the pre-characterising portion of the claim.

522. The parties were agreed that the amendment is intended to introduce a reference to predictive alarms. The question is whether, on EP 539's true construction, it introduces a restriction to predictive alarms, Dexcom's case, or a change to predictive alarms, Abbott's case.

523. Abbott's argument is that the unamended claim did not require a predictive threshold but rather a real-time glucose threshold. On that basis, a system which had only a first real-time alarm and a second predictive alarm would not have infringed. The amendment changes the second threshold from a real-time glucose value to a predictive glucose value. Now that system with a first real-time alarm and a second predictive alarm would infringe.

524. Dexcom submit that the unamended version encompassed a variety of "thresholds" as the second threshold, whether real-time or predictive for, as I understood it, the following two reasons:

i) First Dexcom referred to paragraph [0078] of EP539, which is in the section headed "Predictive Alerts/Alarms". There it identifies "TVp" as "the predictive threshold, e.g. the threshold against which a predicted value is compared." This is one of "three threshold values" referred to in that paragraph. What has changed by the proposed amendments is that the added words now expressly confine matters to that predictive threshold. That is to say it excludes non-predictive thresholds. On this basis, Dexcom submit the amendment is not an extension of protection but a restriction.

ii) Second, Dexcom submitted that the reference in integer 1f to "real time glucose value" does not preclude predictive alerts. As the specification indicates at [0075] "any output signal from any measurement technique may be used for the predictive alerts/alarms described herein".

525. In their Opening, Dexcom acknowledged that the language in integer 1(f) as amended 'is a little ungainly' but submitted that it was 'perfectly clear': the '*real time glucose value'* in question refers to a predicted future real time glucose value, and the claim requires determination, at a given time, of whether the user's real-time glucose value is predicted to meet a second threshold level within the given 'predetermined time frame or horizon' following that given time.

526. There is no question that the specification of EP539 proposes various possibilities including current and predictive alerts, as, for example, in [0078]. But that does not assist in interpreting the claim which is directed to a specific combination and not to every possibility contemplated in the specification. In my view, the interpretation of the unamended claim, integer 1(f) is clear. That integer plainly refers to a current evaluation of the sensor data, giving rise, in integer 1(g) to a current alert or alarm.

527. Thus, EP539 claim 1 as granted is to a system with a continuous analyte sensor including two current alerts. One of the current alerts is settable (integer 1(e)) and the other is fixed (integers 1(f) & (j)).

528. The acknowledgment that the language in the proposed amended integer 1(f) 'is a little ungainly' is an understatement. To refer to a 'predicted future real time glucose value' is an oxymoron. The value must either be evaluated in real time (i.e. it is an evaluation of the current state of affairs) or, as I have pointed out at paragraph 512.xii) above, a predicted future value is calculated based on a number of glucose values (not simply or only the current value) and assessed against the relevant threshold.

529. For all these reasons, I conclude that the proposed amendment does extend the protection of EP539. Abbott's argument, as set out in paragraph 523 above, is correct.

Clarity

530. A patent claim must be "clear and concise": §14(5)(b) of the Patents Act 1977. Abbott contend that the proposed amendments to claim 1 of EP539 result in a claim lacking in clarity for three reasons:

i) First: that it is unclear whether integer 1(f) as amended relates to a predictive threshold or not. However I agree it does indeed relate to a predictive threshold.

ii) Second: that it is not possible to reconcile the requirements of integer 1(f) that a "real time glucose value" meets a second threshold "in a predetermined time frame or time horizon". I agree that this creates a puzzle for the Skilled Person

iii) Third: that the Skilled Addressee would not understand how integer 1(g) relates to integer 1(f). The objection here is largely impenetrable, but it seems to boil down to a complaint that the claim could encompass products with unclaimed as well as claimed features. If so, this is not a clarity issue (or objectionable for any other reason).

531. Dexcom argued that Abbott were able to admit infringement without struggling with the clarity of the claims when doing so. However, the fact that Abbott, in the circumstances of this action, were able to admit infringement does not mean that the Skilled Person, having read EP539, would not be left scratching his or her head as to what this claim meant. It is not difficult to specify whether a threshold is for a current value or for a predicted value. I conclude the proposed amended claim lacks clarity.

VALIDITY

Introduction

532. On validity, Abbott contended that there was a primary issue which arose on each attack and each piece of prior art namely the feature of claim 1 of both patents of a fixed predictive alert in combination with a current, user-settable alert. Abbott contended that feature is disclosed and/or obvious in light of all the prior art. In summary:

i) Each of the patent documents (**Brauker 2007** and **Shariati**) discloses both types of alert, and the possibility of having both types in a single device. Among the natural choices, a particularly obvious choice would be a fixed current alert at 55 mg/dL (~3.0 mmol/L), as in all the Dexcom products on the market, with a predictive alert tied to that value (inter alia because predictive alerts were generally tied to the same threshold as a real time alert).

ii) The **STS-7** had current, user settable alerts for high and low glucose, and a fixed, current low glucose alert at 55 mg/dL (~3.0 mmol/L). It would be an obvious development to add a predictive low glucose alert, tied to that fixed threshold, in the usual way.

iii) The **Navigator** had user settable, current alerts for high and low glucose, with predictive alerts matched to the thresholds set by the user for them. An obvious variant would be to provide for a fixed predictive alarm (e.g. at the 55 mg/dL (~3.0 mmol/L) value used by Dexcom) which worked in the same way as the Navigator's existing alerts (i.e. a current alert fixed at that level, with an associated predictive alert to warn the user when they were headed into unsafe territory).

533. For their part Dexcom disputed the alleged lack of novelty and attacked the obviousness case as driven by hindsight. Hindsight also formed part of their resistance to the novelty attacks since on anticipation, Dexcom made the same point in relation to each citation:

> 'The novelty attacks rely, in summary, on a cobbling together of bits and pieces from the disclosure supplemented by unjustified inference; there is no clear and unambiguous disclosure of all the features of the claims of EP159/539.'

534. For this reason, it is necessary to examine the disclosure in each document with care but before doing so, I must ensure I am oriented correctly.

Applicable principles – novelty.

535. The point I just referred to from Dexcom is, of course, the point made by the TBA in *T/396/89 UNION CARBIDE/high tear strength polymers* [1992] EPOR 312 at para 4.4 (as referred to by Lord Hoffmann's speech in *Synthon's Patent* [2005] UKHL 59 at [23]):

> 'It may be easy, given a knowledge of a later invention, to select from the general teachings of a prior art document certain conditions, and apply them to an example in that document, so as to produce an end result having all the features of the later claim. However, success in so doing does not prove that the result was *inevitable*. All that it demonstrates is that, given knowledge of the later invention, the earlier teaching is capable of being adapted to give the same result. Such an adaptation cannot be used to attack the novelty of a later patent.'

536. Dexcom also reminded me:

i) that the prior art disclosure must 'plant the flag' – i.e. there must be a clear and unambiguous disclosure of all the features of the claim.

ii) of my own observations in *Commscope Technologies LLC v Solid Technologies Inc*, [2022] EWHC 769 (Pat) at [189], which I do not repeat here.

iii) of the dicta of Meade J. in *Fisher and Paykel Healthcare Ltd v Flexicare Medical Ltd*, [2020] EWHC 3282 (Pat):

> '150…The fact that something unmentioned is not expressly ruled out does not mean that it is disclosed, still less to the standard required for anticipation.'

Brauker 2007

537. Brauker 2007 (or simply Brauker) is a US patent application published on 6 September 2007, entitled "*Transcutaneous Analyte Sensor*". It is a long document and much of it is not relevant. Abbott identified a series of 'key passages' to which I refer below. To ensure that the Skilled Team would read all these various extracts together and as disclosing a single system, it is necessary to examine how the various aspects fit together.

538. After some brief introductory paragraphs, the 'Summary of the Invention' in Brauker covers many paragraphs from [0005] to [0103]. The invention is summarised in nine aspects, and each aspect is then described in individual paragraphs as 'an embodiment of the [xth] aspect'.

539. Abbott relied on teaching from the first to fourth aspects, so I will summarise how these aspects are described, starting with the first aspect:

> [0005] In a first aspect, a system for monitoring a glucose concentration in a host is provided, the system comprising a continuous glucose sensor configured to produce a signal indicative of a glucose concentration in a host; and a receiver operably connected to the sensor, wherein the receiver comprises a user interface, and wherein the receiver further comprises programming configured to calibrate the signal, to display a graphical representation of the calibrated signal on the user interface, and to display a directional arrow indicative of a direction and a rate of change of the calibrated signal on the user interface.

540. The second aspect concerns a device and the third aspect a method, for essentially the same purposes. Thus, the second and third aspects both conclude in the same way as the first aspect.

541. In a similar fashion, the fourth to sixth aspects are for a system, a device and a method all concerned with predictive alarms:

> [0033] In a fourth aspect, a system is provided for monitoring glucose concentration in a host, the system comprising a continuous glucose sensor configured to produce a signal indicative of a glucose concentration in a host; and a receiver comprising an alarm, wherein the receiver is operably connected to the sensor, wherein the receiver further comprises programming configured to estimate glucose data for a future time, and wherein the receiver comprises programming further configured to trigger the alarm when the estimated glucose data for the future time is above or below at least one predetermined threshold.

542. I need not discuss the seventh to ninth aspects, because they are concerned with calibration.

543. Once each aspect has been stated, the ensuing paragraphs in the Summary then add additional features. Thus, as Abbott submitted, in relation to the "first aspect" (described at [0005] – [0018]), Brauker 2007 discloses an analyte monitoring system with a user-settable current glucose alarm at [0010] – [0012], and a predictive alarm "when the estimated glucose value for the future time is below a pre-determined threshold" (at [0013] - [0015]).

544. Abbott also correctly identified that the same current and predictive alarms are described in relation to a second and third aspect at [0021] – [0026] and [0028] – [0032], respectively.

545. Amongst the key passages which Abbott relied upon, they then moved to the fourth aspect. At [0035] Brauker 2007 states that "In an embodiment of the fourth aspect, the predetermined threshold [for the predictive alarm] is user-configurable" ([0035]).

546. The Detailed Description starts at [0182], divided by various headings. The first heading is 'Definitions' and it suffices to note the definition of 'clinical risk' in [0234]. In common with the other definitions, it is defined as a broad term, but concludes with an example: '*In one exemplary embodiment, clinical risk is determined by a measured glucose concentration above or below a threshold (for example, 80-200 mg/dL) and/or its rate of change.*' This exemplary range appears many times and is often accompanied by the alternative range of 55-220 mg/dL.

547. I can skip over many of the following headings until 'Dynamic and Intelligent Analyte Value Estimation'. The paragraphs under this heading (which run from [0610]-[0688]) describe various methods/algorithms for estimating predicted glucose values. The next section is headed 'Input and Output' and is mostly concerned with the presentation of the output from the previously described algorithms. As Abbott submitted, at [0689] – [0694] Brauker 2007 provides further detail on predictive alarms. It describes "clinical risk alarms" which involve an alert provided to a patient during a time of existing or approaching clinical risk ([0691-2]) or if there is minimal or no possibility of avoiding the clinical risk ([0694]).

548. [0696] then introduces Fig 41, which looks like this:

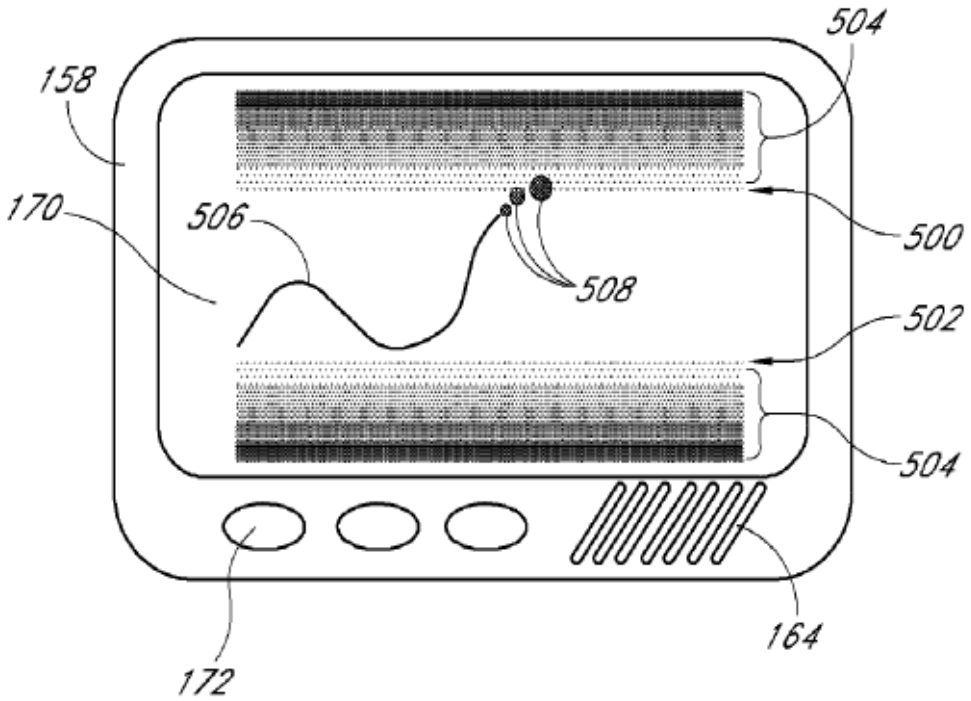


FIG. 41

549. FIG. 41 is stated to be an illustration of the receiver in one embodiment showing an analyte trend graph, including measured analyte values, estimated analyte values, and a zone of clinical risk, in which 500 is a high threshold, 502 the low threshold '*which represent boundaries between clinically safe and clinically risky conditions for patients'*. The clinical risk zones 504 'are illustrated outside of these thresholds'. [0697] continues:

> In one exemplary embodiment, a normal glucose threshold for a glucose sensor is set between about 100 and 160 mg/dL, and the clinical risk zones 504 are illustrated outside of these thresholds. In alternative embodiments, the normal glucose threshold is between about 80 and about 200 mg/dL, between about 55 and about 220 mg/dL, or other threshold that can be set by the manufacturer, physician, patient, computer program, or the like.

550. Similarly the clinical risk zones outside those thresholds can be "*set by a manufacturer, customized by a doctor, and/or set by a user via buttons*" ([0698]).

551. Abbott acknowledge that Brauker does not explicitly state that the thresholds for the clinical risk zones are the same as those used for the clinical risk alarms but submit that would be the skilled reader's understanding. I agree.

552. The central dispute was over the meaning of 'set by the/a manufacturer' in [0697-8].

553. In his written reports, Dr Palerm set out his view that the Skilled Team would read the words 'set by a manufacturer' in those paragraphs to refer to the option that the threshold was fixed and not adjustable, in contrast to the option of customisation by a doctor or user.

554. In cross-examination, Dr Palerm was first asked about the passage in [0035] where it is stated the predetermined threshold is user-configurable. It was put to him that '*you infer that there is an embodiment that is not user-configurable. That's your point, right*?' To which Dr Palerm agreed. Later, he was challenged on his view of [0687-8], on which he maintained his view that 'set by the manufacturer' means/implies fixed.

555. In relation to the word 'set', Professor Oliver took the view that it does not necessarily mean the threshold cannot be set again, pointing to the fact that it does not say 'fixed'. He maintained this view in cross-examination, which showed he made the same point on both Shariati and Brauker. He was not deterred by being reminded of the CGK that there were CGM devices which had a combination of user-settable alerts and alerts that were set/fixed by the manufacturer, as in the STS-7.

556. The issue of what a piece of prior art discloses to the Skilled Person/Team is one for the Court and not the experts. Nonetheless, the issue was well tested in the evidence.

557. For the same reasons as I give in relation to Shariati (see paragraph 569 below), I do not agree that the Skilled Team would read Brauker as Prof Oliver did. In fact, I consider the Skilled Team would see that Brauker was covering every possible option: set by the manufacturer, physician, patient, computer program and/or user includes 'fixed by the manufacturer or physician' but also those situations where the manufacturer sets a default value which can be changed by the physician or user, or

even where no default value is provided and the physician or user are forced to set a threshold. I cannot see any reason why Brauker would have wanted to exclude any of the possibilities.

558. Therefore, I consider Prof Oliver's reading that Brauker is limited to his 'set, with the option to reset' meaning requires a strained reading of the document.

559. It therefore follows, in my judgment that, Brauker discloses user-settable current alarms and fixed-threshold predictive alarms, and the two types of alarms in combination. As Abbott submitted, it therefore discloses the inventive concept of the Dexcom patents.

560. As Abbott submitted, claim 1 of each patent has one or two additional features. As to those:

i) Brauker discloses a mechanism to add temperature compensation to the calculated glucose value at [0432].

ii) At [0712] – [0719], Brauker describes further embodiments in which target values or a range of target values may be displayed. In one example, illustrated in figures 43 – 45, the target values are shown as a box set within a wider range delimited by the thresholds referred to in [0697]. The glucose values are shown as a trace passing through this target zone, so it necessarily shows a range of values. Brauker gives an example of the target range as falling between 80mg/dL and 130mg/dL, which is a narrower range than that mentioned in relation to the current glucose alarms referred to at [0458].

561. I did not understand Dexcom to identify any other features of claim 1 of either Patent which were not disclosed in Brauker. I therefore find that Brauker anticipates both EP159 and EP539 (as amended).

Shariati

562. Shariati is a US patent application published on 30 July 2009, entitled "*Systems and Methods for Processing Sensor Data"*. It is written in the same style as, and much of the disclosure is similar to, Brauker 2007 (including much that is not relevant to this case). Dexcom is identified as the assignee. Abbott identified the key passages they relied upon as follows, along with their submissions:

i) At [0076] Shariati discloses the use of either or both of a current hypoglycaemia alarm and predictive hypoglycaemia alarm.

ii) At [0352], Shariati describes providing audible alerts during a time of "*existing or approaching clinical risk*" – current and predictive alerts.

iii) Paragraphs [0356] – [0364] describe these predictive "*clinical risk*" alarms in similar terms to paragraphs [0689] – [0694] of Brauker 2007 referred to above. The thresholds for the boundaries for clinical risk "*can be set by the manufacturer, physician, patient, computer program and the* like", and the clinical risk zones outside these boundaries "*can be set by a manufacturer, customised by a doctor, and/or set by a user via buttons*". As is the case for Brauker 2007, this is a clear disclosure that these boundaries would be the

thresholds for the predictive clinical risk alarms, and that Shariati was disclosing that the thresholds could be either set by the manufacturer (i.e. fixed) or customised by a doctor or user.

iv) Shariati further describes predictive hypoglycaemia and hyperglycaemia alarms at paragraphs [0566] – [0571]. At [0571] Shariati explains that the predictive alarms are triggered when the predicted glucose value passes a threshold. It states that the threshold "*can be* programmed *into the computer or user selectable*".

563. This is where the main dispute arose. Abbott submitted this presents two options to the skilled team: either fixing the threshold (by programming it into the computer), or making it user selectable. Language such as "*programmed into the computer or user selectable*" can only be referring to the two options of fixed and user-settable thresholds respectively, because there is only one alternative to "*user selectable*", namely "*fixed*". Abbott's position was supported by Dr Palerm's evidence. As on Brauker, his view was not shaken in cross-examination.

564. Professor Oliver interpreted the expression differently, in effect that both options were user selectable.

565. In cross-examination, Prof Oliver accepted that Shariati was referring to two alternative approaches. But it became clear that two matters underpinned Prof Oliver's view:

i) First, he maintained his view on the basis of the use of 'programmed' in the FreeStyle Navigator Guide (2008) where, in context, it is clear that the threshold values can be programmed in the receiver for any individual. The user is given a high degree of choice for their FreeStyle Navigator. For example, all alarms can be switched off, and the user is given detailed instructions as to how to set, review or change all the levels for the various alarms.

ii) Second, he read 'set' as not precluding a 'reset' and that it does not specifically say 'fixed'. On this basis, all of the examples he advanced of thresholds "*programmed into the computer*" were "*user selectable*".

566. Abbott submitted that Prof Oliver's interpretation is completely untenable, contending it ignores the fact that Shariati is self-evidently referring to these two well-known options: (i) fixed by the manufacturer, (ii) settable by the user. There is no reason why a skilled team would treat what is there said in any other way. It makes no sense to read "*programmed into the computer*" as referring to a user selecting a desired threshold when "*user selectable*" is provided as the alternative.

567. In his written evidence, Dr Palerm considered the two options to be true alternatives. The challenge in cross-examination was based on the STS-7 Users Guide (2007) which, by way of example, talks of 'your programmed alert levels. Your default high and low glucose alerts are set at 80mg/dL and 200mg/dL but can be changed to fit your personal diabetes goals (see Section 7.1).' Dr Palerm said that any user-settable glucose alert has a default value which can then be changed by the user if necessary.

568. Having listened carefully to Professor Oliver's answers in cross-examination, at the conclusion of his evidence I asked him about a passage in Shariati at [0363]. My

question was posed in the context of Shariati's abstract identifying that Shariati claimed systems and methods for calibrating a continuous analyte sensor. I asked him whether he could identify any reason why Shariati would have wanted to exclude fixed [predictive] alarms as working with their calibration method (since that was the point in dispute). In answer, he referred to what he had already said about anxieties about where the fixed threshold would be and what that would mean in terms of risk-benefit for the user, but agreed there was no explicit exclusion in Shariati.

569. I am entirely satisfied that the Skilled Team reading Shariati would not have the use of 'programmed' in the FreeStyle Navigator Guide or STS-7 Guide in mind. Instead, they would read the ordinary language and conclude Shariati was presenting two alternatives: either the threshold is programmed into the computer (fixed) or user selectable (from a range of values). This covers all the possibilities, and I am unable to find any reason why Shariati would have wanted to exclude the possibility of a fixed threshold (whether for a current or a predictive alarm).

570. In summary, in my view, Shariati discloses (inter alia) user-settable current alarms and fixed-threshold predictive alarms, and the two types of alarms in combination. It therefore discloses the inventive concept of the Dexcom patents.

571. Dr Palerm also explained that Shariati discloses the temperature correction feature claimed in EP159, and his evidence on that point was not challenged.

572. Dexcom did not identify any other points of distinction. Accordingly, I conclude that Shariati anticipates both EP159 and EP539 (as amended).

Alleged Obviousness

573. In case I am wrong on Brauker and Shariati, I proceed to determine Abbott's case of obviousness.

Applicable principles – Inventive Step

574. Dexcom characterised obviousness as the central dispute on these patents. They accept that the inventions are relatively simple and straightforward to implement once they have been described. Their answer to the obviousness attacks is that the unimaginative skilled team reading Shariati, Brauker, the Navigator Guide, or the STS-7 Guide in October 2012 simply would not have arrived at a CGM system with a user settable current hypoglycaemia alarm and a fixed-threshold predictive hypoglycaemia alarm.

575. Dexcom reminded me of the following points in the authorities, none of which were disputed and I accept them.

576. The approach is that set out in the decision of the Supreme Court in *Actavis v. ICOS* [2019] UKSC 15 at [52] – [73], with its endorsement at [62] of the statement of Kitchin J as he then was in *Generics v. Lundbeck* [2007] EWHC 1040 (Pat) at [72]. Obviousness should be addressed at the level of the generality of the claims, see *Shenzehn Carku v NOCO* [2022] EWHC 2034, [78].

577. Dexcom drew particular attention to the following points from *Actavis*:

i) First, that it is trite that the mere fact that the skilled addressee could, without technical difficulty, have taken an allegedly obvious step based on the prior art cannot render an invention obvious. It is not necessary to show that the skilled addressee would actually press ahead and physically implement the invention – as this may depend on a host of non-technical considerations – but the idea needs to be one which would occur to the uninventive skilled addressee as a technical solution. This is a multifactorial and fact-sensitive question: see e.g. Actavis v ICOS at [63].

ii) Thus, while it is well-established that the existence of one obvious route does not itself diminish the obviousness of other routes, the context in which the skilled addressee is working is important – see Actavis v ICOS at [69]:

> '… the existence of alternative or multiple paths of research will often be an indicator that the invention contained in the claim or claims was not obvious. If the notional skilled person is faced with only one avenue of research, a "one way street", it is more likely that the result of his or her research is obvious than if he or she were faced with a multiplicity of different avenues. But it is necessary to bear in mind the possibility that more than one avenue of research may be obvious. In Brugger v Medic-Aid Ltd (No 2) [1996] RPC 635, 661, Laddie J stated:
>
> > "[I]f a particular route is an obvious one to take or try, it is not rendered any less obvious from a technical point of view merely because there are a number, and perhaps a large number, of other obvious routes as well."
>
> I agree. As a result, the need to make value judgments on how to proceed in the course of a research programme is not necessarily a pointer against obviousness.'

578. There is a difference between cases in which expectation of success is in issue and cases where the question is simply whether the idea is obvious. In *Schering-Plough v Norbrook Laboratories* [2006] FSR 18 at [35], Floyd J:

> "An invention may simply consist in an idea which, once it has been conceived, is one which will obviously work. For those cases a party attacking the patent only needs to show that the idea was an obvious one. But there are other cases where the invention involves something more than the bare idea, because it is not immediately apparent that the idea could be made to work. In these cases the attacking party needs to show something more: that it was obvious to have the idea and to try it to see whether it would work."

579. In cases where it is obvious that an idea will work, the invention resides in the idea alone, not in any perceived difficulty of enablement (see also *Rovi Guides, Inc v Virgin Media Limited* [2015] EWCA Civ 781 per Floyd LJ at [18]).

580. The Court of Appeal in *Teva v Leo* [2015] EWCA Civ 779 at [29] emphasised the importance of assessing the question of obviousness by reference to what real-life skilled people would think and do.

581. When considering that question the presence of uncertainty and unfamiliarity is relevant. That is because it can be, not so much the presence of challenges that puts people off trying but the absence of firm knowledge and experience that means the conception of modifying a piece of prior art would not come readily to mind. See Lord Justice Jacob in *Unilever v Chefaro* [1994] R.P.C. 567 at 587; applied by Meade J. In *Fisher and Paykel Healthcare Ltd v Flexicare Medical Ltd* [2020] EWHC 3282 (Pat) at [47].

582. Expanding on that point, Dexcom submitted that an idea is inherently more likely to suggest itself to the skilled addressee if his or her mind is already "primed" to appreciate the benefits which it may deliver; conversely, if the skilled addressee's mind is not "primed" – or is actually attuned to problems with which the idea might be associated – then it is less likely that the idea will occur at all. In *Unilever Plc v Chefaro Proprietaries Ltd* [1994] RPC 567, Jacob J (as he then was) considered at p.587 three technical reasons put forward by the patentee as to why a particular step had not been taken before, all of which were dismissed by the defendant as "paper tigers". The Judge held:

> 'I think there is something in these points. It is not so much that they would put people off trying: it is that without firm knowledge and experience that particulate labels will travel, will not agglomerate or stick, the conception of their use does not come readily to mind.'

583. When seeking to avoid hindsight it is important not to allow it to infiltrate the problem which the skilled addressee is deemed to be dealing with when they consider the prior art. While, as discussed above in relation to EP223, it is perfectly acceptable to proceed on the basis that the skilled addressee picks up the prior art with a problem which is part of the CGK in mind (and when it is not suggested that identifying that problem forms any part of the inventive concept of the patent), it is important that the skilled addressee is not given artificial pointers to specific aspects of the prior art's disclosure.

584. The CIPA Guide gives further a useful illustration of way that "signal" becomes deceptively easy to extract from "noise" when the circumstances which led up to an event are viewed with hindsight at §3.40:

> 'A classic warning against unintended but inevitable hindsight appears in a book by Diane Vaughan, The Challenger Launch Decision (University of Chicago Press, 1996) at 69-71. It is referred to, inter alia, by Roy Marsh, "The Continuing PSA debate" [2010] CIPA 59. Professor Vaughan explains that a problem that was ill-structured becomes well-structured after an event (in that instance a disaster, but equally the making of an invention), as people look back and reinterpret information ignored or minimised prior to the event that afterward takes on new significance. Information strung together in post-event accounts can present a coherent set of signals that was

> not characteristic of the situation as it existed prior to the event. The result can be a systematic distortion of history that obscures the meaning of events and actions as it existed and changed for the participants in the situation at the time the events and actions occurred. (Professor Vaughan's emphasis) Making an invention is by definition an ill-structured problem whereas the task of examination of a patent application or deciding on an objection of lack of inventive step against a granted patent is a well-structured problem because the invention has become known. There is the same risk of deriving a coherent set of signals where none existed prior to the invention. Even the selection of a primary reference may be a product of hindsight and risks distorting history in the manner suggested by Professor Vaughan.'

585. I accept all these points, and the point made by Professor Vaughan in relation to the Challenger disaster is a useful addition to ensure we guard against hindsight creeping into an obviousness analysis.

586. Dexcom's final point was that where an idea is said to be obvious the question of why it has not been done before is a relevant consideration, see Jacob LJ in *Technip France SA's Patent* [2004] EWCA Civ 381, [2004] RPC 46 at [122]:

> "The question 'why was it not done before' is always a powerful consideration when considering obviousness, particularly when all the components of a combination have been long and widely known."

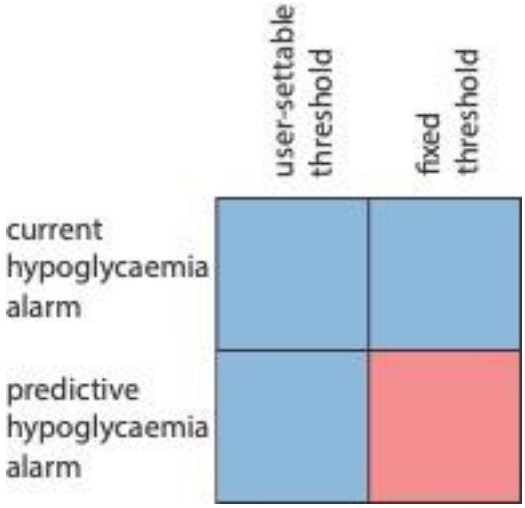
587. Abbott made no particular submissions on the legal principles, contending these patents called for a straightforward application of the well-known principles.

588. Thus, a critical aspect of this case so far as Dexcom was concerned, was establishing the correct context against which the unimaginative Skilled Team read and considered the prior art.

Dexcom's hindsight case

589. Dexcom developed what at first sight appeared to be a powerful hindsight attack on Dr Palerm's approach to these Patents. Since it applies across the board, it is convenient to summarise this attack here.

590. Dexcom submitted that Dr Palerm's evidence in chief effectively boiled the options available to the Skilled Team down to a 2x2 grid:



591. It was common ground that all but one of the boxes in this grid (blue) were notionally "ticked" – *i.e.* present in CGK commercial devices – at the priority date. Dr Palerm's argument was essentially that it was obvious to tick the fourth (red) box.

592. Dexcom submitted that hindsight infected this approach in several ways:

i) First, thinking about the problem in terms of a small "grid" of alarm combinations is intrinsically hindsight-driven. Its starting point is that the skilled person is thinking about which combinations of user settable / fixed / current / predictive hypoglycaemia alarms to use. It ignores every other avenue of potential improvement to the prior art which the skilled addressee would have perceived, cutting straight to the chase: the claims of EP159/539. Dr Palerm did this consciously – excluding options from consideration in his evidence that he did not think were relevant to EP159/539.

ii) Secondly, the presentation of the available options as four possible combinations lacks any consideration of the significance of the fact of combination – the considerations which arise in using a fixed threshold in conjunction with a *current* hypoglycaemia alarm are different from those which would arise in the context of a *predictive* hypoglycaemia alarm.

iii) Thirdly, Dr Palerm's extensive experience of post-2012 commercial CGM devices – most of which have since ticked the red square in the grid – meant that he already knew that the red grid square represented a useful and viable option; but he neither acknowledged nor took steps to guard against this.

iv) In cross-examination, a good deal of time was taken up getting Dr Palerm to agree that he knew of relevant features of post-2012 devices, but I observe that this would have been the case of any appropriately qualified expert, unless they happened to have retired from the industry completely at or around the 2012 priority date.

v) Dr Palerm agreed that, when going through the materials presented to him for this case, he was reminded of at least two products, the Libre 2 and the Dexcom G6, which included precisely the combination of alarms claimed in these Patents.

593. Dexcom criticised Dr Palerm for not acknowledging in his written evidence the risk of hindsight. They also submitted that he had taken as his starting point the particular combination of alarms and thresholds disclosed in the Patents (cf. the 2x2 grid). Counsel put to him and he agreed, a variety of other options. He said he did not discuss all these other options in his report because to have done so would have added a lot of material not directly relevant to these Patents.

594. The force of all Dexcom's criticisms of course depend on the particular circumstances. If the invention involved a significant departure from the prior art, and if hindsight has to be used to get to the invention, that is determinative. But the hindsight card can also be played in situations where the invention was obvious.

STS-7 Guide

Disclosure

595. As already noted, the STS-7 Guide is the user guide for Dexcom's STS-7 device, published in 2007, and it is common ground that the STS-7 device itself and the user guide would be CGK.

596. As Abbott submitted, the STS-7 Guide is very similar to the STS Guide which I have analysed in the context of EP627. The key points of relevance to the Dexcom patents are the high and low glucose alarms and alerts:

i) The STS-7 Guide describes low and high glucose alerts at page 30. The thresholds for these alerts are user settable to fit the user's "*personal diabetes goals*". They can also be turned off entirely. Their purpose is said to be to notify the user when their glucose readings are out of their "*target range*".

ii) In addition to the user-settable alerts, the STS-7 Guide describes an automatic "Low Glucose Alarm", which is a current glucose alarm with a fixed threshold set at 55mg/dL. This alarm cannot be turned off or changed, and is said to be provided "*for safety*".

iii) There is a distinct approach to notifications associated with the low and high glucose alerts and the Low Glucose Alarm: the latter automatically provides a further set of alerts if the user remains below the fixed 55mg/dL value after 30 mins.

Obviousness of a predictive fixed alert

597. The only difference between the STS-7 and the alleged inventive concept of these Patents is the fact that this product did not have a predictive alarm. As noted above, Dexcom was a bit behind others in actually introducing predictive alarms (of any kind) into its products. However, Abbott submitted that any skilled person looking at the STS-7 device as described in the STS-7 Guide would appreciate at once the usefulness of adding this feature to it, for the following reasons:

i) Predictive alarms were known and featured in several CGM devices at the priority date. The skilled team would have considered Dexcom's devices to be

unusual in this respect. Including a predictive alarm in any CGM device would therefore be an obvious option.

ii) In considering the threshold to use in implementing the predictive alarm the natural and obvious way of proceeding would be to tie it to the same threshold as a current glucose alarm – that is how it was done in other products (Navigator). In the context of the STS-7, it would be obvious to add a predictive alarm with the same threshold as the (user-settable) low glucose alert or the (fixed) Low Glucose Alarm or both.

iii) Both options would be sensible design choices. However, the well-known benefit of a predictive alarm is its ability to give advance warning of an undesirable condition, allowing preventative action to be taken. This has particular benefit if the advance warning relates to a threshold of clinical danger, as in the Low Glucose Alarm. Dr Palerm explains that the rationale for such a fixed threshold is that it is set at a level that represents a risk of serious harm. Prof Oliver agrees that the Low Glucose Alarm is a "*safety net to prevent hypoglycaemia, in particular for people with impaired awareness of hypoglycaemia*". And he notes that at a glucose level of 55mg/dL (the threshold of the Low Glucose Alarm) there is already established danger. It would therefore be a natural and obvious choice for the skilled team to add a predictive alarm tied to the same fixed threshold as the Low Glucose Alarm in the STS-7.

598. The only reason Prof Oliver advanced to suggest that this would not be an obvious way of proceeding is his insistence on a "mindset" on the part of his "Skilled Clinician" that would set them against the use of fixed, rather than user-settable thresholds, against the use of predictive alarms due to concerns over accuracy, and against adding additional alarms due to concerns over alarm fatigue. I agree with Abbott that there was no evidence to support the existence of such a mindset within real skilled teams at the priority date. Prof Oliver's views were directly at odds with the evidence of what real teams and real devices were doing at the priority date:

i) The use of a fixed threshold alarm set at 55mg/dL on all generations of Dexcom devices from the STS onwards.

ii) The use of predictive alarms in nearly all major CGM devices aside from those of Dexcom (although it eventually came late to the party with the G6 in 2018).

iii) The trend exhibited in devices of both Dexcom and Medtronic of adding more, not fewer, alarms and alerts with each subsequent generation of their CGM devices.

599. Professor Oliver's evidence on mindset fell apart in cross-examination. All he could say of his supposed "mindset" was that it "*may*" or "would" lead the clinician to advise the team to focus on accuracy rather than a fixed predictive alarm as a first priority. Even then, the lack of conviction was clear when he said that it "*is not necessarily entirely obvious that it is the next important step*".

600. No-one who was an actual product designer could say that there was a "mindset" against fixed threshold alarms when these featured in some of the leading products in the market.

601. The position is no different in relation to Brauker/Shariati even if I am wrong that they explicitly disclose a fixed predictive alarm.

Navigator Guide

Disclosure

602. This is the user guide for Abbott's FreeStyle Navigator CGM device, published in 2007. As with the STS-7, it is common ground that both the Navigator device and the user guide would be CGK.

603. Abbott argued that the key points were as follows:

i) The Navigator Guide describes high and low glucose alarms and projected (i.e. predictive) high and low glucose alarms.

ii) The high and low glucose alarms are current glucose alarms with a user settable threshold. The projected low and projected high are predictive alarms said to provide an "early warning of an event that is likely to occur if the current trend continues". The threshold for the projected low and high alarms is tied to the same threshold as the low and high glucose alarms.

iii) The thresholds for both alarms can be set within a range of 60mg/dL – 300mg/dL. They are described as not intended to notify the user of "*severe hypoglycaemia*" or *"severe hyperglycaemia*".

iv) The Navigator Guide also describes glucose targets, which are "*different from the low and high glucose alarms*". This target range is shown as a shaded horizontal region on a line graph showing the user's actual glucose values.

v) The Navigator Guide also describes a working temperature range, indicating that it has a temperature sensor. Dr Palerm's evidence is that this would imply the presence of a mechanism to correct for temperature, which he says that the skilled team would be aware as a matter of CGK in any case.

Obviousness of a fixed predictive alert

604. Thus the only difference between the Navigator and the inventive concept of the Dexcom patents is that the Navigator does not include a predictive alarm with a fixed, rather than a user-settable, threshold. Abbott submitted it would be obvious for the skilled team to include a fixed threshold predictive alert in a CGM device, in light of the Navigator Guide:

i) The Navigator only provides a single threshold for high and low glucose alerts, which is set by the user.

ii) While a user-settable threshold has the advantage of enabling the patient to tailor the alert to their own needs, it does not provide the additional safety of a fixed alarm that is guaranteed to be triggered if the user's glucose hits a danger level.

iii) It would therefore be obvious for the skilled team to add a hypoglycaemia alarm with a fixed threshold corresponding to a level of clinical danger, such as the 55mg/dL Low Glucose Alarm that the skilled team would know was provided in the STS and STS-7.

iv) Having decided to implement such a low glucose alarm, the skilled team could either do so as a current glucose alarm, or retain the approach already used in the Navigator of current and predictive alarms tied to the same threshold. The latter option would be obvious and indeed a particularly attractive option for the reasons explained above in relation to the STS-7.

605. As Abbott pointed out, Prof Oliver accepted that adding a fixed predictive alarm would be entirely straightforward to implement, but that his only answer to the case that it would be entirely obvious to do so was his reliance on a "mindset" against using a fixed threshold for hypoglycaemia.

606. Again, since I have found there to be no mindset, I accept Abbott's analysis.

Other features of the claims

EP159, integer 1(d) – temperature correction

607. The use of a conversion function to correct for the effect of temperature on glucose sensor readings was CGK at the priority date. It is disclosed in Brauker and Shariati. Prof Oliver accepted that including such a function would have been standard practice for CGM devices at the priority date.

EP539, integer 1(h) – different outputs for indicators

608. This integer simply requires that the indicator for the predictive alert is different from the indicator for the current alert. It is obvious, if not inevitable, that a device with both alerts in operation would indicate to the user which of them had been triggered. Prof Oliver did not suggest otherwise.

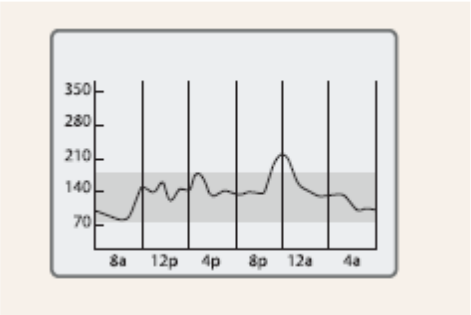
EP539, integers 1(k)-1(l), visual target range

609. Dexcom's amendment to claim 1 would add the following integers at the end:

1(k)	*wherein the processor module is configured to visually display a glucose target range with a high target boundary and a low target boundary on a user interface, and*
1(l)	*wherein the low target boundary visually displayed is different from the first threshold and wherein the high target boundary visually displayed is different from a third threshold (TV1) associated with a hyperglycemic indicator, such that the range between the first and third thresholds is wider than the range between the low and high target boundaries.*

610. This requires the device to display upper and lower boundaries delimiting a target range, which are different from upper and lower thresholds used for high and low glucose

alarms. This was done in the Navigator in the following way (see p119 of the Navigator Guide):



611. The target range is shown by the shaded region, displayed alongside a user's glucose trend data. The boundaries for the target region were different from the thresholds of the Low and High Glucose Alerts. Prof Oliver acknowledged that this feature in the Navigator satisfies the requirements of integers 1(k) and (l) of EP539.

612. Dr Palerm's view is that this feature is also disclosed by Brauker. Prof Oliver disputed this and quibbled over Dr Palerm's interpretation of the relevant passages in the prior art (although as noted at paragraph 560.ii) above he accepted that the embodiment shown in figure 45 of Brauker does show a target zone). Prof Oliver did not suggest that the visual display features conferred any inventiveness or offer any challenge to Dr Palerm's view that they do not.

613. In any event, this was a feature of a CGK device. On that basis, Abbott submitted there can be no invention at all in adopting it for a device developed from any of the pleaded prior art starting points. I agree.

Dexcom's arguments against obviousness

614. As mentioned above, one of Dexcom's points was to pose the question: if the particular combination of alarms claimed in these Patents was obvious, why did no one use that combination before? Dexcom pointed out that in the 12 commercial CGM systems marketed over the more than 13 years between the first such product and the priority date, not one used the claimed combination of alarms. Dexcom sought to reinforce the point by pointing out that this combination first appeared in the Freestyle Libre 1 (although a flash glucose monitor and not a 'true' CGM device), but the first true CGM device to use the combination was the Dexcom G6 in 2018.

615. However, the evidence made it clear that designers in this field operated under a number of constraints. As well as the regulatory constraints, designers had to keep in mind that the users of their existing systems could be put off adopting a new device if radically different to the one they were used to. Developments were preferably incremental. Furthermore, different companies followed different design tracks. Yet further, the evidence established that the time between design idea and marketing of a new CGM system featuring that idea could be lengthy.

616. In my view, all these points robbed the question of any significance in the particular circumstances of this case.

617. Dexcom also relied on:

i) the number of pieces of prior art relied upon by Abbott in relation to these Patents; and

ii) the variety of routes to obviousness pursued by Abbott.

618. However, the underlying point is that I was persuaded that the Skilled Team effectively had a wide range of options for alarms from which they could choose their particular selection. The selection might well be influenced by existing and previous products from their Team/their employer; the features of competitive products; the desire to have points of distinction, as well as all the other influences – regulatory, ease of use, etc. The wide range of choice did not, however, result in the claimed combination being inventive, in my view.

619. It is appropriate to return also to mention Dexcom's other arguments against obviousness, including in particular the hindsight attack on Dr Palerm's evidence. I kept all these in mind when assessing the allegation of lack of novelty and obviousness of these Patents and reaching provisional conclusions on each allegation over each piece of prior art. The conclusions stated above are no longer provisional but final. Notwithstanding Dexcom's hindsight attack (which on its own appears powerful, provided CGK matters are ignored), I have concluded it has no force in the circumstances of these Patents.

Insufficiency

620. This was pleaded as a conventional squeeze on obviousness. Abbott pointed out that in so far as Dexcom were running a 'mindset' case, EP159 and EP539 offer the skilled reader no reason why a fixed predictive alert is appropriate (or more appropriate than a user-settable one) despite the supposed thinking of the skilled reader. The supposed drawbacks are not addressed at all (let alone solved). Nor is any assistance given in selecting what threshold to use, or for making a more accurate CGM, nor any reasoning as to why a predictive alert is appropriate despite the achievable level of accuracy. If (as Dexcom contended) the skilled person would not contemplate a fixed predictive alert, <u>prior</u> to reading the patents, they would not do so <u>after</u> reading the patents either – with the result, so Abbott contended, that the patents would make no technical contribution and would be insufficient. I think it is fair to say that the insufficiency plea has served its purpose and I need say no more about it.

OVERALL CONCLUSIONS

621. Here I summarise the result on each Patent.

622. For the reasons explained above, I find EP627 anticipated by the STS Guide, but not obvious over Bunte. If valid, the Dexcom devices would have infringed.

623. Claim 1 of EP223 is anticipated by Gejdos but is not obvious over Lebel. Dexcom's Gillette argument fails. If Claim 1 is invalid, claims 7/9 are obvious. If EP223 were valid, then on my construction, Dexcom would not infringe but on the alternative construction, Dexcom would have infringed.

624. On EP539 I find the proposed unconditional amendments not allowable because they extend the protection and also on the ground of lack of clarity.

625. EP539 as amended and EP159 are anticipated by each of Brauker and Shariati. Even if I am wrong about that, those Patents were obvious over each of Brauker, Shariati, STS-7 Guide and the Navigator Guide. If either Patent had been valid, infringement was admitted.