

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

In re *Inter Partes* Review of:

U.S. Patent No. 10,375,222

DECLARATION OF DR. SAYFE KIAEI, PH.D.

Table of Contents

I.	Introduction.....	1
II.	Background and Qualifications	2
III.	Materials Reviewed	7
IV.	Relevant Legal Standards	8
V.	Technology Background.....	10
VI.	Overview of U.S. Patent No. 10,375,222	14
	A. Summary	14
	B. Prosecution History	15
	C. Level Of Ordinary Skill In The Art.....	18
	D. Claim Construction.....	19
VII.	Overview of the Prior Art.....	19
	A. Yarger (Ex. 1005).....	19
	B. Love (Ex. 1006).....	22
	C. Hernandez-Rosas (Ex. 1007).....	23
	D. Chivallier (Ex. 1008).....	25
VIII.	The Asserted Grounds Of Invalidity	26
	A. Ground 1: The Challenged Claims Are Rendered Obvious By Yarger In View Of Love	26
	1. A POSITA Would Have Been Motivated to Combine Yarger and Love and Would Have Reasonably Expected Success in Doing So.	26
	2. Independent Claim 14	29
	3. Claim 15	46

4.	Claim 16.....	47
5.	Independent Claim 18.....	48
6.	Claim 19.....	53
7.	Claim 20.....	54
B.	Ground 2: The Challenged Claims Are Rendered Obvious By Hernandez-Rosas In View Of Chivallier	55
1.	A POSITA Would Have Been Motivated to Combine Hernandez-Rosas and Chivallier and Would Have Reasonably Expected Success in Doing So.....	56
2.	Independent Claim 14.....	59
3.	Claim 15.....	82
4.	Claim 16.....	86
5.	Independent Claim 18.....	88
6.	Claim 19.....	94
7.	Claim 20.....	95
IX.	Availability for Cross-Examination	96
X.	Right To Supplement.....	97
XI.	Conclusion	97

I. INTRODUCTION

1. I, Sayfe Kiaei, Ph.D., declare as follows.

2. I have been retained as a technical consultant on behalf of Abbott Diabetes Care Inc. (“Abbott” or “Petitioner”), who I understand is the petitioner in the present proceeding. I have been asked to consider whether the references listed as Exhibits 1005-1008 below disclose or render obvious the limitations recited in claims 14–16 and 18–20 of U.S. Patent No. 10,375,222 (Ex-1001, “’222 patent”). I have also been asked to consider the state of the art and the prior art available before the time of the alleged invention of the ’222 patent. My opinions are provided in this declaration.

3. To the best of my knowledge, I have no financial interest in Petitioner. I have been informed that a company known as DexCom, Inc. (“DexCom” or “Patent Owner”) purports to own the ’222 patent. To the best of my knowledge, I have no financial interest in DexCom and, to the best of my recollection, I have had no contact with DexCom or the named inventors of the ’222 patent, Aditya Mandapaka, Jorge Valdes, Jeffrey R. Wedekind, Eric Cohen, Douglas William Burnette, Francis William Pascual, Hari Hampapuram, Mark Dervaes, and Michael Robert Mensinger. To the best of my knowledge, I similarly have no financial interest in the ’222 patent. To the extent any mutual funds or other investments that I own have a financial interest in the Petitioner, the Patent Owner, or the ’222 patent, I am not aware of,

nor do I have control over, any financial interest that would affect or bias my judgment.

4. I am being compensated at my standard consulting rate for my time. My compensation is in no way contingent on the results of these or any other proceedings relating to the '222 patent.

II. BACKGROUND AND QUALIFICATIONS

5. A description of my professional background and qualifications is provided below. An additional account of my work experience and qualifications is included in my curriculum vitae, which is labeled as Appendix A. My qualifications are stated more fully in my curriculum vitae, which is attached. Below is a summary of my education, work experience, and other qualifications.

6. I earned a Ph.D. in 1987 from Washington State University in Electrical, Computer, and Energy Engineering. From 1985 through 1987, while working toward my Ph.D., I worked with Boeing on the development of signal processing and control systems.

7. From 1987 through 1993, I was a tenured Professor at Oregon State University in the Electrical and Computer Engineering Department.

8. From 1993 to 2002, I was a Senior Member of Technical Staff with the Wireless Technology Center and Broadband Operations at Motorola Inc., where I

was responsible for the development of wireless system, cellular system, RF integrated circuits, GPS, and Digital Subscriber Lines (DSL) transceivers.

9. Since 2001 I have held the position of Motorola Endowed Chair Professor in Analog and Radio Frequency Integrated Circuitry at the School of Electrical, Computer, and Energy Engineering at Arizona State University in Tempe, Arizona. I am also the Director of the National Science Foundation Center, Connection One. Connection One is an industry/university cooperative research center with over thirty industrial members and five university members focused on developing sensors, electronics, bioelectronics, and wireless technologies.

10. At Arizona State University, I have developed and taught courses on Wireless communication, RF Transceivers, Electronics, Bio-Electronics, VLSI, Analog IC design, RFIC, communications, and related areas. In my over thirty years of academic experience, I have taught university courses and done research in electronics, RF and wireless system, bioelectronics, networking, communication systems, and sensors.

11. I have graduated over 100 M.S. and Ph.D. students working under my supervision on their thesis, and many of them are professors in academia, or have senior positions in the industry. Currently, I have M.S., Ph.D., and postdoc students working with me in my lab on research related to communication and networking systems, wireless systems, electronics, sensors, biosensor, etc. My research is funded

by various sources, including industry, federal agencies including NSF, DARPA, ONR, DOE, and other agencies.

12. I have published over two hundred journal and conference papers covering topics such as integrated circuits (IC), wireless systems, power management, low-power electronics, sensors, radio frequency, filter design, and related areas. A list of my publications can be found in my CV, attached as Exhibit A. I also have over 10 patents and patent applications in electronics, RF, and low-power bioelectronics.

13. I have researched in the biosensors related to glucose monitoring, sensors for hearing aid, body position sensors, wireless medical implanted sensors, neuronal sensors, and related areas funded by DARPA, NSF and other agencies. I received research funding for Glucose sensor using Amperemeter and for determining Glucose levels from saliva. I have also worked on number of consulting projects related to NFC and capturing data from the Glucose meter sensors. I received funding from NSF and developed a wireless vital signal detection using Bluetooth signal for heart and breathing monitoring and have published papers and patent in this area. I received research funding to develop wireless shoe insole sensor sensing the pressure in the foot for body movement monitoring. The data was sent wireless to the nearby communication device (mobile phone) using Bluetooth. I also

developed a custom IC chip for Wireless Medical Implanted Circuit (MICS) for in-body sensors such as Glucose sensors.

14. I am an IEEE Fellow, a distinction and the highest level of IEEE membership awarded by the IEEE directors to recognize a high level of demonstrated extraordinary accomplishments. The IEEE is the Institute of Electrical and Electronics Engineers, the world's largest association of technical professionals whose objectives include the educational and technical advancement of electrical and electronic engineering, telecommunications, computer engineering, and related disciplines. I am a member of the IEEE Circuits and Systems Society, IEEE Solid State Circuits Society, and IEEE Communication Society, IEEE RF and Microwave committees, IEEE International Symposium on Low Power Electronics and Design (ISLPED), IEEE Signal Processing Society, IEEE Fellow Selection Committee, and many other International Electrical Engineering societies. I was one of the key organizers to establish the IEEE Radio Frequency Integrated Circuits (RFIC) symposium in 1995, and IEEE International Symposium on Low Power Electronics and Design (ISLPED) in 1997.

15. I have been on the executive committee, and technical committee of RFIC and ISLPED for the last 16 years. The RFIC and ISLPED Symposia have grown and is now the premier international symposium in the world where the latest

RF, low-power electronics, wireless, and bio-electronic circuits, and components are presented.

16. I have received several awards including the Carter Best Teacher Award, the IEEE Darlington Award (which is given for the best technical paper on circuits and systems in the IEEE Circuits and Systems Society), and the Motorola 10X Rapid Design Cycle Reduction Award.

17. I have been one of the key organizers of the IEEE International Symposium on Low Power Electronics and Design (ISLPED) since 1997. I have published papers and organized sessions on techniques for low-power cellular phones at ISLPED. I have published a number of papers on the design and development of low-power RF, wireless transceivers, sensors, and low-power bioelectronics.

18. I have also been a consultant on various projects with Intel (designing 2G, 3G mobile telephone transceivers, Internet-of-Things (IOT), and sensors), Texas Instrument (developing 3G cellular and Bluetooth technologies), Sony Wireless (developing GPS technologies), Tektronics (designing wireless systems), Medtronics (body sensors, glucose monitoring, MICS) and various other consultancies. During my work in industry, I have designed and contributed to the design of many systems for commercial products.

19. I am not an attorney and offer no legal opinions, but in the course of my work, I have had experience studying and analyzing patent claims from the perspective of a person skilled in the art.

III. MATERIALS REVIEWED

20. I am not an attorney and offer no legal opinions, but in my work, I have had experience studying and analyzing patents and patent claims from the perspective of a person skilled in the art.

21. In preparing this declaration, I reviewed the '222 patent, including the claims of the patent in view of the specification, and I have reviewed the prosecution history of the '222 patent and numerous prior art and technical references from the time of the alleged invention. More specifically, I have reviewed each of the following:

Exhibit	Description
1001	U.S. Patent No. 10,375,222 (the "'222 patent")
1002	File History for U.S. Patent No. 10,375,222
1005	U.S. Pub. 2014/0313052A1 ("Yarger")
1006	U.S. Pub. 2015/0207796A1 ("Love")
1007	U.S. Pub. 2015/0123810A1 ("Hernandez-Rosas")
1008	U.S. Pub. 2010/0045425A1 ("Chivallier")
1009	NFC Forum, Bluetooth® Secure Simple Pairing Using NFC, (Jan. 9, 2014)
1010	T. Zhang, Bluetooth Low Energy for Wearable Sensor-based Healthcare Systems, 2014 Health Innovations and Point-of-Care Technologies Conference, Seattle, Washington USA, October 8-10, 2014
1011	H. Omre, Bluetooth Low Energy: Wireless Connectivity for Medical Monitoring, Journal of Diabetes Science and

Exhibit	Description
	Technology Volume 4, Issue 2, March 2010, Diabetes Technology Society
1012	E. Strommer, Application of Near Field Communication for Health Monitoring in Daily Life, Proceedings of the 28th IEEE EMBS Annual International Conference New York City, USA, August 30-September 3, 2006
1013	J Padgette et al, Guide to Bluetooth Security, NIST Special Publication 800-121, Revision 1, 2012
1014	Excerpts from Bluetooth Specification Core v.1.2, November 2003
1015	Excerpts from Bluetooth Specification Core v.4.0, June 2010

IV. RELEVANT LEGAL STANDARDS

22. I am not an attorney. For the purposes of this declaration, I have been informed about certain aspects of the law that are relevant to forming my opinions. I have applied the following understanding of the law:

23. I have been informed that a patent claim may be “anticipated” if each element of that claim is present either explicitly or inherently in a single prior art reference, and that the elements should be arranged in the reference as in the claim. Petitioner’s counsel has informed me that for a claimed limitation to be inherently present, the prior art need not expressly disclose the limitation, so long as the claimed limitation necessarily flows from a disclosure in the prior art.

24. I have been informed that a patent claim can be considered to have been obvious to a person of ordinary skill in the art at the time the application was filed. This means that, even if all of the requirements of a claim are not found in a single

prior art reference, the claim is not patentable if the differences between the subject matter in the prior art and the subject matter in the claim would have been obvious to a person of ordinary skill in the art at the time the application was filed.

25. I have been informed that a determination of whether a claim would have been obvious should be based upon several factors, including, among others:

- the level of ordinary skill in the art at the time the application was filed;
- the scope and content of the prior art; and
- what differences, if any, existed between the claimed invention and the prior art.

26. I have been informed that a single reference can render a patent claim obvious if any differences between that reference and the claims would have been obvious to a person of ordinary skill in the art. Alternatively, the teachings of two or more references may be combined in the same way as disclosed in the claims, if such a combination would have been obvious to one having ordinary skill in the art. In determining whether a combination based on either a single reference or multiple references would have been obvious, it is appropriate to consider, among other factors:

- whether the teachings of the prior art references disclose known concepts combined in familiar ways, and when combined, would yield predictable results;

- whether a person of ordinary skill in the art could implement a predictable variation, and would see the benefit of doing so;
- whether the claimed elements represent one of a limited number of known design choices, and would have a reasonable expectation of success by those skilled in the art;
- whether a person of ordinary skill would have recognized a reason to combine known elements in the manner described in the claim;
- whether there is some teaching or suggestion in the prior art to make the modification or combination of elements claimed in the patent; and
- whether the innovation applies a known technique that had been used to improve a similar device or method in a similar way.

27. Petitioner's counsel has informed me that one of ordinary skill in the art has ordinary creativity and is not an automaton. Petitioner's counsel has informed me that in considering obviousness, it is important not to determine obviousness using the benefit of hindsight derived from the patent being considered.

V. TECHNOLOGY BACKGROUND

28. Bluetooth is a standardized protocol for low-power, short-range, wireless communication. The development of the Bluetooth standard started in the mid 1990s when a number of wireless industries formed the Bluetooth Special Industry Group ("SIG") for short range wireless communication operating in the

unlicensed 2.4 GHz ISM band. The first Bluetooth 1.0 standard was published in July 1999. Bluetooth versions 1.0-1.2 only supported data rates up to 1 megabit per second (Mbps), and is known as BT classic or BT Basic Rate (BR). Bluetooth version 2.0, released in 2004, added an Enhanced Data Rate (EDR) mode, supporting data rates up to 3 Mbps and throughput of approximately 2.1 Mbps. *See* Ex. 1013, Section 2.

29. Bluetooth version 4.0 was released in 2009 and added a new “Low Energy” mode (aka Bluetooth Low Energy or BLE). BLE introduced significantly lower power consumption, reduced memory requirements, added efficient discovery and connection procedures, included shorter packet lengths, and simplified protocols and services. Ex. 1013, Section 2.1.2. A summary of the key differences between Bluetooth 1.0/2.0 and 4.0/BLE is below:

Table 2-2. Key Differences Between Bluetooth BR/EDR and LE

Characteristic	Bluetooth BR/EDR	Bluetooth LE
RF Physical Channels	79 channels with 1 MHz channel spacing	40 channels with 2 MHz channel spacing
Discovery/Connect	Inquiry/Paging	Advertising
Number of Piconet Slaves	7 (active)/255 (total)	Unlimited
Device Address Privacy	None	Private device addressing available
Max Data Rate	1–3 Mbps	1 Mbps via GFSK modulation
Encryption Algorithm	E0/SAFER+	AES-CCM
Typical Range	30 meters	50 meters
Max Output Power	100 mW (20 dBm)	10 mW (10 dBm)

Ex. 1013, Table 2-2.

30. Bluetooth communication provides security measures both at the application layer and the link layer and uses authentication and encryption routines.

Bluetooth devices use security and authentication to verify the identity of communicating devices based on their Bluetooth device address. For example, both the classic Bluetooth standards, and the Bluetooth 4.0/BLE standard have specific security requirements for authentication, pairing, and encryption. See Ex. 1013, Section 3; Ex. 1014 (Excerpts from the Bluetooth Specification v. 1.2) at Volume 2, Part C, Section 4.2 and Part H; Ex. 1015 (Excerpts from the Bluetooth Specification v. 4.0) at Volume 1, Part A, Section 5, Volume 2, Part H, Volume 3, Part C, Sections 5 and 10. This prevents information compromise caused by eavesdropping and only authorized devices can access and view transmitted data.

31. Bluetooth communication has been widely used for medical applications. The table below shows exemplary applications of classic Bluetooth and Bluetooth low energy used in medical applications as of 2014, including for measuring glucose.

TABLE II: Commercial Available Healthcare Devices Using Bluetooth Low Energy*

Product name	Functionalities	Data aggregator	Company	System Review and Critical Analysis
UP 24 [14]	Monitoring posture and activities tracking sleep and wake up time	Android 4.3 (or later) and iOS (6.0 or later)	Jawbone	The system is a in a waistband shape and has multiple functions
Smart Blood Pressure Monitor [15]	Monitoring Blood Pressure	iPhone 5	Withings	Measure blood pressure in one gesture and display results in an iphone
Heart Rate Sensor [16]	Monitoring heart rate with ECG sensors	iPhone 4S (or later)	Polar	Provide heart rate monitoring and training applications
Kinetic inRIDE Watt Meter	Measuring heart rate, cadence, speed and distance	iPhone 4S (or later)	Kinetic by Kurt	The Heart rate zones in the phone shows heart rate and total time training
ditto Bluetooth LE	Measuring glucose	Android 4.3 (or later) and iOS (6.0 or later)	Biomedtrics	Sync data with several compatible FDA approved blood glucose meters
Training Shoes [17]	Measuring gait related parameters	iPhone 4S (or later)	Nike	The shoe features an embedded sensor in the sole
Fitness Socks	Measuring gait related parameters	Android 4.3 (or later) and iOS (6.0 or later)	Sensoria	The socks are light weight and convenient to wear
Wireless EEG headset[18]	Monitoring EEG signal	Android 4.3 (or later) and iOS (6.0 or later)	Imec et. al	The wireless low power EEG is convenient to wear
Body patch[18]	Monitoring ECG signals	Android 4.3 (or later) and iOS (6.0 or later)	Imec et. al	The ECG can have up to 3 leads
Finger Pulse Oximeter [19]	Measuring SpO2	iOS (6.0 or later)	Nomin Medical	The pulse oximeter can provide feedback if not positioned correctly
EMG2Go [20]	Measuring EMG signals	Android 4.3 (or later) and iOS (6.0 or later)	Texas Instruments	It is designed to measure EMG, but can also measure EEG and EGO

*The content of the table is from various company websites. The summary of the products is from our own knowledge. Our opinion does not reflect the opinion of the manufactures.

Ex. 1010 (T. Zhang, Bluetooth Low Energy for Wearable Sensor-based Healthcare Systems, 2014 Health Innovations and Point-of-Care Technologies Conference, Seattle, Washington USA, October 8-10, 2014).

32. For Glucose monitoring, use of a secure channel and authentication is critical in order to ensure that data is sent only to other devices approved by the user.

Ex. 1011 (Journal of Diabetes Science and Technology Volume 4, Issue 2, March 2010 © Diabetes Technology Society).

33. Near Field Communication (NFC) technology is another standardized protocol developed for short-range wireless communication in consumer electronics, mobile devices, and sensors. The NFC Forum was formed in 2004 to standardize the use and interoperability of NFC technology. NFC evolved from earlier RFID technology widely used since the 1990s for contactless identification. NFC uses inductive coupling and initiates communication by bringing the devices in close proximity to each other. Thus, the range of NFC communication is very short, with a range of about 10 cm or less. NFC achieves data rates on the order of a few tens of kilobits per second.

34. NFC has inherent security advantages due to its very short range of communication. Because the inductive signals dissipate after only a few centimeters, the risk of interception or eavesdropping of the NFC communication by other unauthorized devices is greatly reduced. Due to these security advantages, NFC was

commonly used for many years prior to 2016 to assist with the initial setup and pairing of longer-range wireless communications. For example, the NFC Forum published an Application Document in 2014 detailing how to use NFC for initial pairing and setup of Bluetooth connections, including BLE connections. Ex. 1009.

35. NFC has been applied in many fields including health monitoring and glucose monitoring. Ex. 1012 (E. Strommer, Application of Near Field Communication for Health Monitoring in Daily Life, Proceedings of the 28th IEEE EMBS Annual International Conference New York City, USA, August 30-September 3, 2006).

VI. OVERVIEW OF U.S. PATENT NO. 10,375,222

A. Summary

36. The '222 patent relates to continuous monitoring of analyte values received from an analyte sensor, including continuous glucose monitoring (CGM) systems. Ex. 1001 at 1:18–21.

37. The patent explains that because the analyte sensor is implanted in the skin of a user, the battery life of the analyte sensor and transmitter acting in conjunction with it is a concern. *Id.* at 1:58-61. In order to conserve battery life or to increase the power efficiency, the patent explains that “transmissions may, for example, need to be intermittent,” which “can introduce reliability issues.” *Id.* at

1:61-65. Therefore, “[i]n some cases, reliability is thus sacrificed for battery life in conventional sensor systems.” *Id.* at 1:66-67.

38. The ’222 patent purports to improve reliability and battery life by describing “a method for wireless communication of analyte data” that “establish[es] a first connection between an analyte sensor system and a display device,” and involves “exchanging information related to authentication” and “transmitting an encrypted analyte value to the display device.” *Id.* at 2:1-15.

B. Prosecution History

39. The ’222 patent was filed as U.S. Patent Application No. 15/651,310 on July 17, 2017, claiming priority to U.S. Provisional Application No. 62/364,771 dated July 20, 2016.

40. For the purposes of this declaration, I have been instructed to assume the effective filing date of the ’222 patent is July 20, 2016.

41. The initial claims were directed to wireless communication during two intervals, the first interval during which the devices would exchange “information related to authentication” using a first wireless protocol, and a second interval during which the devices would transmit encrypted analyte data using a second wireless protocol. The original claims lacked any limitations directed to alerts and alarms, as seen for example in original claim 14, below.

WHAT IS CLAIMED IS:

14. A method for wireless communication of analyte data, the method comprising:
during a first interval, using a first wireless protocol to perform an exchange of information related to authentication information with a display device; and
during a second interval, bypassing the exchange of information related to authentication by using a second wireless protocol to transmit an encrypted analyte value to the display device, wherein the encrypted analyte value has been generated using the information related to authentication, and wherein the first wireless protocol is different than the second wireless protocol.

Ex 1002 at 221-222.

42. On October 3, 2017, the Examiner issued a rejection of all claims as obvious over U.S. Pub. No. 2013/0331036 A1 (“Baker”) in view of U.S. Pub. No. 2003/0050009 A1 (“Kurisko”), and further in view of U.S. Pub. No. 2016/0048827 A1 (“Corbalis”) and U.S. Pub. No. 2016/0066129 A1 (“Seidenberg”). *Id.* at 231-243. The Examiner found that Baker teaches the first protocol (NFC), second protocol (Bluetooth), and the authentication/bypass-related limitations, Kurisko “teaches a method wherein the value is encrypted,” Corbalis “teaches a method wherein at least a portion of the encrypted analyte value is transmitted to the display device in one or more advertisement messages transmitted by the analyte sensor system” and “a method wherein the second wireless protocol is Bluetooth Low Energy,” and Seidenberg “teaches a method wherein the application key was received by the display device from a server.” *Id.*

43. In response to the obviousness rejections, DexCom amended claim 14 to recite “measuring a level of analyte values in a host using a continuous analyte sensor of an analyte sensor system” and argued that Baker and Kurisko did not disclose or suggest amended claim 14. *Id.* at 254-263. Similarly, DexCom amended claim 18 to recite “a continuous analyte sensor configured to measure a level of analyte values in a host.” *Id.* at 257. DexCom did not further distinguish the dependent claims over Corbalis or Seidenberg. *Id.* at 254-263.

44. On June 15, 2018, the Examiner rejected the claims as obvious over the previously cited prior art further in view of U.S. Pub. No. 2015/0087232 A1 (“Sloan”), which “teaches a method [*sic*- of measuring a level of analyte values] wherein [said] measuring [uses] a continuous analyte sensor of an analyte sensor system.” *Id.* at 269-283.

45. On August 21, 2018, DexCom further amended the claims to recite “and not initiating transmission of analyte values to the display device if the determination indicates that authentication was not performed during the first interval.” *Id.* at 322-332.

46. On December 31, 2018, the Examiner rejected the claims again as being obvious over the previously cited prior art further in view of U.S. Pub. No. 2016/0250490 A1 (“Hoffman”), which “teaches a method not initiating transmission

of analyte values to the display device if the determination indicates that the authentication was not performed during the first interval.” *Id.* at 337-351.

47. Finally, on April 24, 2019, DexCom further amended the claims to recite the alert limitations:

AMENDMENTS TO THE CLAIMS 14. (Currently Amended) A method for wireless communication of analyte data, the method comprising: measuring ~~a level of~~ analyte values in a host using a continuous analyte sensor of an analyte sensor system; during a first interval, using a first wireless protocol to perform an exchange of information related to authentication ~~information~~ with a display device; ~~and~~ <u>performing a determination whether one or more alerts indicative of a medical condition of the host is to be triggered based on the measured analyte data;</u> <u>triggering at least one alert and providing a notification on the display device when the determination indicates that the at least one alert is to triggered indicative of the medical condition of the host;</u> during a second interval, bypassing the exchange of information related to authentication by using a second wireless protocol to transmit an encrypted analyte value to the display device, wherein the encrypted analyte value has been generated using the information related to authentication, and wherein the first wireless protocol is different than the second wireless protocol, and ~~not neither~~ initiating transmission of analyte values to the display device <u>nor providing a notification on the display device when the information related to</u> ~~if the determination indicates that the authentication was not performed exchanged~~ during the first interval.
--

Id. at 358-369.

48. The Examiner then issued a Notice of Allowance, and the '222 patent subsequently issued on August 6, 2019. *Id.* at 393-394; 433-434.

C. Level Of Ordinary Skill In The Art

49. A POSITA as of the claimed priority date would have had a Bachelor's degree in biomedical engineering, electrical or computer engineering, computer

science, or a related or equivalent field and two or more years of experience researching, developing, designing and/or evaluating (or supervising the same) in wireless communication related to medical devices or equivalent experience. A person with less or different education but more relevant practical experience, or vice versa, may also meet this standard. The prior art also evidences the level of skill in the art.

D. Claim Construction

50. I understand that in this proceeding, the claims should be construed in accordance with their ordinary and customary meaning in light of the specification, as understood by one of ordinary skill in the art.

51. For purposes of my opinions, I have been asked to assume that each claim term should be given its plain and ordinary meaning in light of the specification, and I have therefore applied those plain and ordinary meanings in my analysis.

VII. OVERVIEW OF THE PRIOR ART

A. Yarger (Ex. 1005)

52. U.S. Pub. 2014/0313052A1, titled “Near Field Telemetry Link for Passing a Shared Secret to Establish a Secure Radio Frequency Communication Link in a Physiological Condition Monitoring System” to Yarger et al. (“Yarger”), was filed on December 14, 2012, and published on October 23, 2014. Ex. 1005 at Cover.

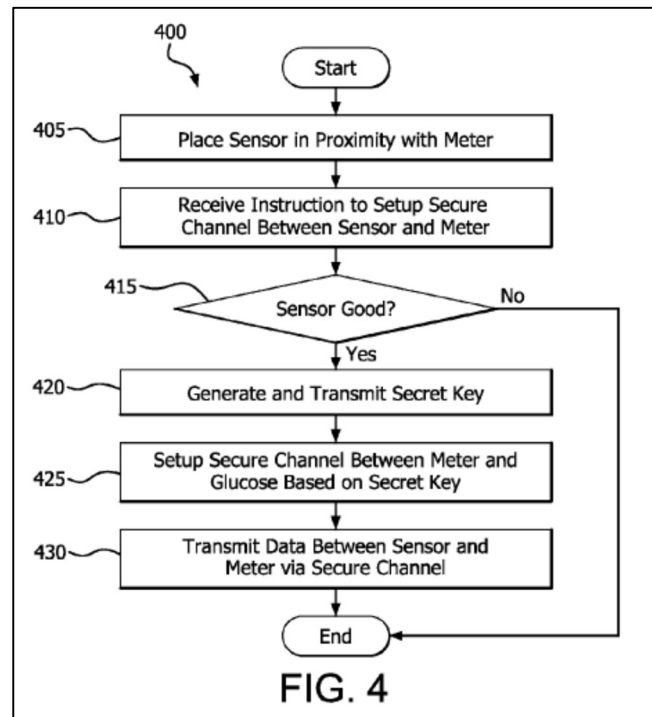
It is thus prior art to the '222 patent under at least 35 U.S.C. §§ 102(a)(1) and (a)(2) (AIA). Yarger was not cited or considered during prosecution of the '222 patent.

53. Yarger discloses methods for securely transmitting encrypted analyte values over an authenticated wireless communication link between an analyte sensor system such as a CGM and a condition meter that acts as a display device. For example, Yarger discloses:

A physiological condition monitoring system (e.g., a continuous glucose monitoring system) includes a physiological condition meter and a physiological condition sensor. The physiological condition meter and the physiological condition sensor are placed in proximity to exchange a secret key using a near field wireless link, which is used to encrypt data to secure a radio frequency (RF) wireless channel.

Ex. 1005 at Abstract.

54. Yarger further discloses that authentication of the wireless communication link can be achieved by “exchanging a secret key” via NFC communication¹ and that “data is encrypted using the secret key.” *Id.* at [0006].



Id. at Fig. 4.

¹ As I explained above, the use of NFC for pairing and setup of a separate Bluetooth link was well known in the industry, as evidenced by a 2014 application document from the NFC Forum stating that “NFC can simplify the process of authenticated pairing between two Bluetooth devices by exchanging authentication information over an NFC link.” Ex. 1009 at 7.

55. Yarger further discloses that “[a]fter both the glucose meter and glucose sensor have identical secret keys, the glucose sensor and glucose meter setup a secure wireless channel that is different from the NFC link.” *Id.* at [0036]. In addition, Yarger discloses that the device may “verify that the secret key was successfully received before transmission of glucose measurement data over the secure wireless link.” *Id.*

B. Love (Ex. 1006)

56. U.S. Pub. 2015/0207796A1, titled “Systems, devices, and methods for authentication in an analyte monitoring environment” to Love et al. (“Love”), was filed on December 17, 2014 and published on July 23, 2015. Ex. 1006 at Cover. It is thus prior art to the ’222 patent under at least 35 U.S.C. §§ 102(a)(1) and (a)(2) (AIA). The patent that issued from Love was cited in an IDS during prosecution of the ’222 patent, but the Examiner never cited Love in any rejection during prosecution of the ’222 patent.

57. Love is directed to the authentication of devices within analyte monitoring systems, which can include a sensor device as well as a reader/display device for communicating with the sensor device. Ex. 1006 at Abstract. The reader/display device “can be configured to output alarms, alert notifications, glucose values, etc., which may be visual, audible, tactile, or any combination thereof.” *Id.* at [0070]. Accordingly, “the information may be utilized by the user to

determine any necessary corrective actions to ensure the analyte level remains within an acceptable and/or clinically safe range.” *Id.* at [0078].

C. Hernandez-Rosas (Ex. 1007)

58. U.S. Pub. 2015/0123810A1, titled “Systems and Methods for a Continuous Monitoring of Analyte Values” to Hernandez-Rosas et al. (“Hernandez-Rosas”), and assigned to DexCom, was filed on November 5, 2014 and published on May 7, 2015. Ex. 1007 at Cover. It is thus prior art to the ’222 patent under at least 35 U.S.C. §§ 102(a)(1) and (a)(2) (AIA). DexCom did not identify Hernandez-Rosas to the PTO, nor was Hernandez-Rosas was cited or considered during prosecution of the ’222 patent.

59. Hernandez-Rosas is directed to systems and methods for secure wireless communication of continuous glucose data between an analyte sensor system and a display device. Ex. 1007 at Abstract. The method includes storing identification information associated with a transceiver of the analyte sensor system, authenticating the transceiver based on the identification information and transferring data to the transceiver. *Id.* at [0007]. Hernandez-Rosas further discloses that “[d]uring the first wireless communication session 410, an authentication procedure needs to be performed as part of a data connection process 414.” *Id.* at [0149].

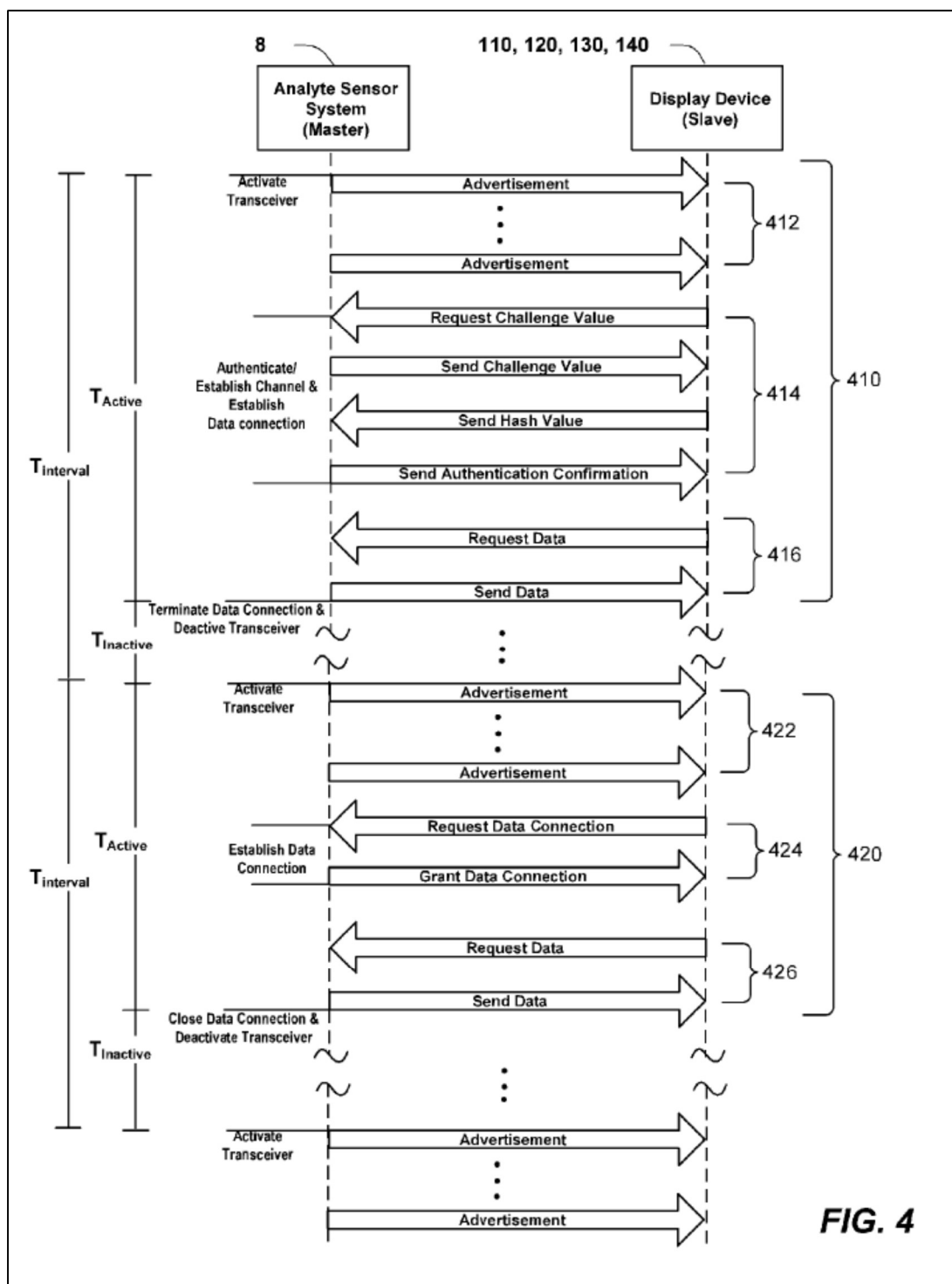


FIG. 4

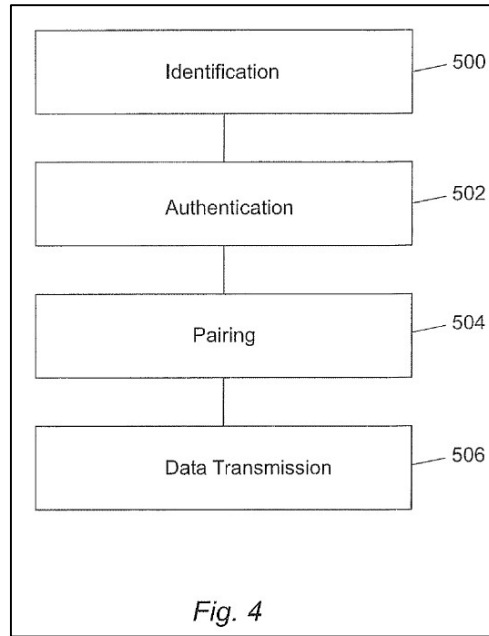
Id. at Fig. 4.

60. Hernandez-Rosas further discloses alerts, including “a hypoglycemic alert [that] may include alert conditions indicating a minimum glucose level.” *Id.* at [0107]. These alerts may be transmitted to a display device. *Id.* at [0106].

D. Chivallier (Ex. 1008)

61. U.S. Pub. 2010/0045425A1, titled “Data Transmission of Sensors” to Chivallier et al. (“Chivallier”), was filed on August 21, 2008 and published on February 25, 2010. Ex. 1008 at Cover. It is thus prior art to the ’222 patent under at least 35 U.S.C. §§ 102(a)(1) and (a)(2) (AIA). Chivallier was not cited or considered during prosecution of the ’222 patent.

62. Chivallier is directed to a method for data transmission between a sensor module and a display device, using a security key to authenticate the sensor module. Ex. 1008 at Abstract. The sensor system, according to Chivallier, uses a wireless connectivity module to provide wireless connection of the sensor with another device, using Near Field Communication or other wireless protocols. Ex. 1008 at [0016]-[0017].



63. Further, Chivallier discloses that “the bio-sensor can effectively provide an alert if the analysis provides a critical result for the health of the patient.” Ex. 1008 at [0002].

VIII. THE ASSERTED GROUNDS OF INVALIDITY

A. Ground 1: The Challenged Claims Are Rendered Obvious By Yarger In View Of Love

64. As shown below, claims 14–16 and 18–20 of the ’222 patent would have been obvious based on Yarger in view of Love.

1. A POSITA Would Have Been Motivated to Combine Yarger and Love and Would Have Reasonably Expected Success in Doing So.

65. Yarger describes a CGM system that uses a near-field communication (NFC) channel to exchange a secret key between a glucose sensor device and a display device, and, after validating that exchange, using a second wireless link to

transmit encrypted glucose measurement data from the sensor to the display device. Ex. 1005 at Abstract, [0006], Fig. 4, [0032]-[0037]. Yarger discloses that its CGM system can be used to monitor for “physiological conditions,” such as glycemic conditions, e.g., as part of a “diabetes management system.” *Id.* at Abstract, [0053].

66. Yarger further discusses monitoring Glucose levels to avoid dangerous conditions and avoid potentially dangerous hyper- glycemia or hypoglycemia and to help the user lower their average blood sugar levels over time. *Id.*, [0003].

67. A POSITA would thus have understood the importance of notifying the user of changes in their glucose levels and alerting them if they are approaching clinically significant glucose threshold levels. *Id.* at [0053] (noting the system can additionally be used in combination to monitor for urgent critical conditions such as arrhythmia, heart failure, and seizures, among others).

68. Love discloses a CGM system in which a display device receives encrypted data over a wireless link, decrypts it, and determines whether to display an alert or alarm to the user “based on a determined rate of glucose change, programmed clinically significant glucose threshold levels (e.g., hyperglycemic and/or hypoglycemic levels), and current analyte level ...” Ex. 1006 at [0078]. Love discloses that its system can be used with a number of different reader devices and wireless protocols. *See, id.* at [0018] (“A number of communication protocols can be used with the embodiments described herein.”), [0019] (“A number of types of

reader devices can be used with the embodiments described herein.”). Love thus does not limit the types of wireless links it can be used with, nor does it limit the particular structure of the display/reader devices its notifications and alarms could be used with.

69. Yarger and Love both disclose CGM systems with secure wireless communication with a display device and thus are both in the same field as the '222 Patent.

70. It would have been obvious to incorporate Love's threshold determination and alerts into CGM system of Yarger so that the modified system would alert the user before reaching clinically significant analyte levels.

71. A POSITA would have been motivated to adopt the notifications and alarms of the reader device (i.e., display device) in Love in the CGM system of Yarger in order to achieve Yarger's stated goal of providing for monitoring of glucose levels, including clinically significant conditions, in particular as part of a “diabetes management system.” Ex. 1005 at [0053].

72. Combining Yarger and Love would have been combining prior art elements (Yarger's CGM system with encrypted wireless communication between a glucose sensor and a display device with Love's alarms and notifications presented on the display device) according to known methods to yield predictable results (i.e., a CGM with a display device that provides alerts and notifications to a user of

significant glucose levels prior to reaching hyperglycemic and/or hypoglycemic levels). Combining Yarger and Love would also have been a use of a known technique (i.e., Love's audible or visual alerts and notifications) to improve similar devices in the same way (i.e., utilizing a CGM reader device with a display to monitor glucose levels to avoid hyperglycemic and/or hypoglycemic levels as part of a diabetes management system).

73. A POSITA would have had a reasonable expectation of success with adopting the notifications and alarms of Love in the CGM system of Yarger. Yarger's CGM meter device has a display that already displays glucose levels. Ex. 1005 at Fig. 2. Adding Love's notifications and alarms functionality to Yarger's CGM meter device would simply require routine programming of the meter device to compare the current glucose levels which it already receives and displays, against preset thresholds, and depending on the outcome of such a comparison, displaying a notification or alert on the existing display. In my opinion, a POSITA could have implemented such alert functionality in tens of lines of source code, and could complete the programming and testing within a few hours.

2. Independent Claim 14

74. The combination of Yarger and Love renders obvious claim 14 as a whole.

a) 14[Pre] “A method for wireless communication of analyte data, the method comprising”

75. Yarger discloses the preamble, to the extent it is limiting.

76. Yarger discloses a method for wireless communication of analyte data, specifically glucose data, using a CGM system: “Generally, the CGM system 100 comprises a glucose meter 105 and a glucose sensor 110. In operation, the glucose meter 105 and the glucose sensor 110 communicate by a radio frequency (RF) wireless link.” Ex. 1005. at [0016]; *see also id.* at Abstract, [0001], [0006] (describing the CGM system “transmitting measurement data to the physiological condition meter from a physiological condition sensor via a secure wireless link”), [0017] (referring to an “analyte such as glucose”).

b) 14[a] “measuring analyte values in a host using a continuous analyte sensor of an analyte sensor system;”

77. Yarger discloses this limitation.

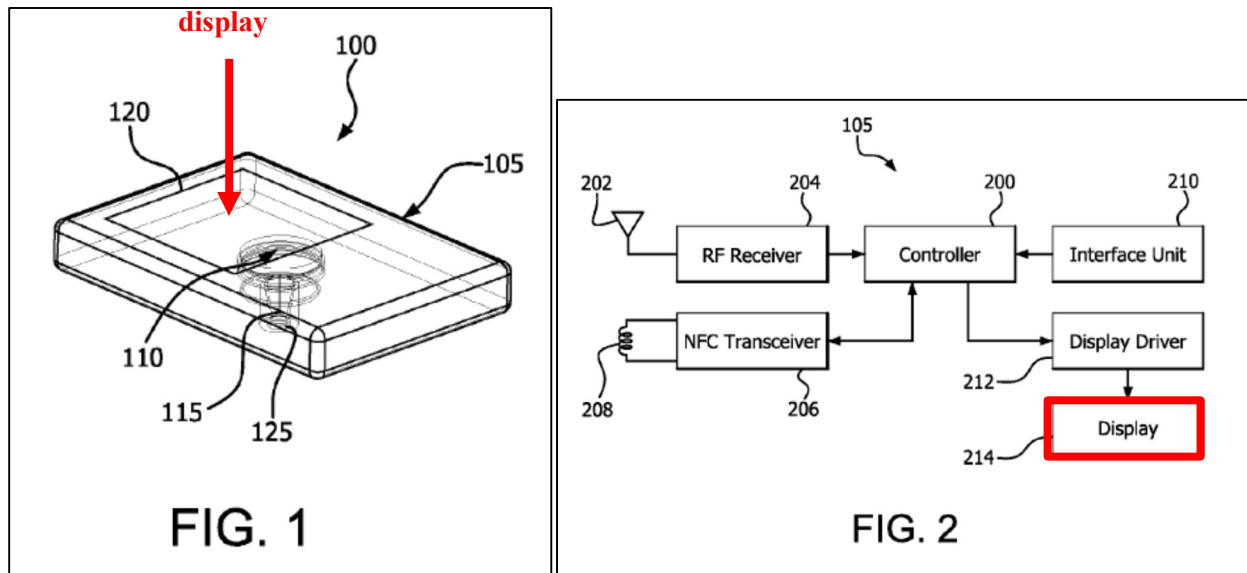
78. Yarger discloses measuring analyte values, such as glucose, in a CGM system 100 that: “comprises a glucose meter 105 and a glucose sensor 110.” Ex. 1005 at [0017]; *see also id.* at Abstract, [0001] (describing “a continuous glucose monitoring system”), [0003] (“A continuous glucose monitor (CGM) is an electronic system that measures and displays glucose level in a user’s body.”).

c) 14[b] “during a first interval, using a first wireless protocol to perform an exchange of information related to authentication with a display device;”

79. Yarger discloses this limitation.

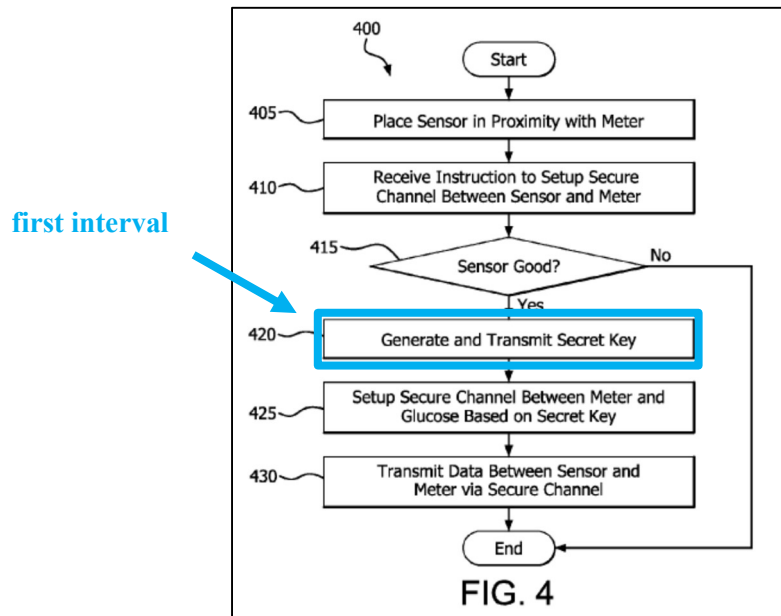
80. Yarger discloses using a first wireless protocol (i.e., near field communication or NFC) to perform pairing, including an exchange of information related to authentication with a CGM's glucose meter (i.e., a display device), during a first interval. Specifically, Yarger discloses a “near field telemetry link for passing a shared secret to establish a secure radio frequency communication link in a physiological condition monitoring system (e.g., continuous glucose monitoring system).” Ex. 1005 at [0014]; *see also id.* at [0018], [0022]-[0023], [0032]-[0033], [0035].

Yarger discloses that its CGM meter device 105 comprises a display 120/214:



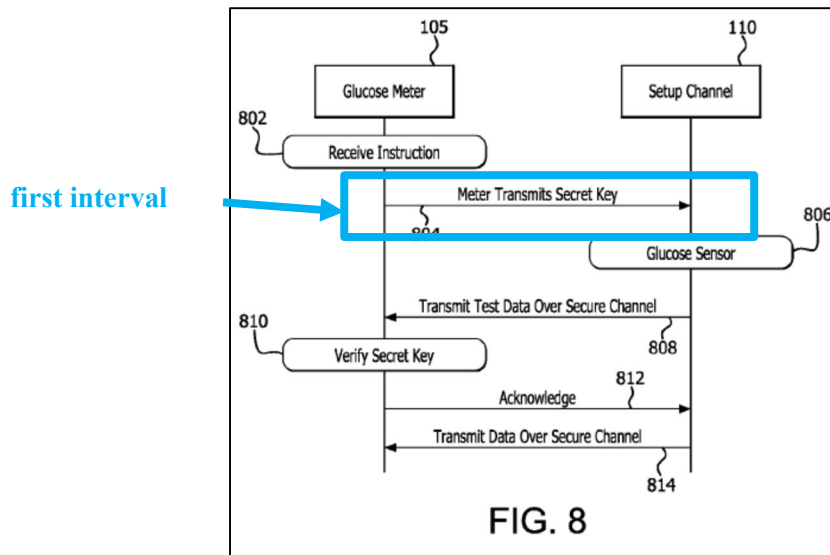
Id. at Fig. 1 (annotated), Fig. 2 (annotated), [0017] (“meter 105 includes any suitable display 120 to provide graphical and/or textual information to the user, such as the user's current glucose level.”), [0027] (similar for display 214).

81. As depicted in Fig. 4, Yarger discloses that one of the CGM sensor or CGM meter generates a pseudo-random “secret key” and transmits it to the other device over an NFC link in step 420 (annotated below):



In the event that the sensor succeeds in the determination at block 415, the example *process 400 generates a secret key and transmits the secret key over the NFC link* so that both the glucose sensor and the glucose meter share the same secret key at step 420. In one example, the secret key is generated by any suitable random process for securing a wireless link. For example, the example process 400 may implement a *cryptographically secure pseudorandom number generator to generate a 128-bit secret key*.

Id. at Fig. 4 (annotated), [0035]. This is also reflected in, for example, Fig. 8, which depicts an embodiment where the CGM meter (*i.e.*, the display device) transmits the secret key to the CGM sensor.



Id. at Fig. 8 (annotated), [0046]-[0047]; *see also id.* at Figs. 5-7. Yarger further discloses that this “pairing” operation allows the meter/display device 105 and the sensor device 110 to exchange “cryptographic keys and identifying information” via the NFC link.

The **pairing operation** mentioned above allows ***the durable device(s) 105 and consumable devices 110 to exchange cryptographic keys and identifying information*** that ensures that subsequent communication between the devices 110 and 105 is secure. The pairing operation itself, however, is vulnerable to attack. If the pairing is compromised, the security of subsequent operations may also be compromised. By ***using an inductive coupling link to perform certain steps of the pairing operation***, however, the security of the transaction is greatly increased because of the unlikelihood of the short-range, relatively nonstandard inductive coupling transmission being correctly received and decoded.

Id. at [0051]; *see also id.* at [0050] (inductive coupling link used “in lieu of the

normal RF link ... for the purpose of initial synchronization and pairing.”).

82. **Error! Reference source not found.**As discussed above, Yarger’s secret key can be a random number, *id.* at [0035], and the initial “pairing” operation involves an exchange of this secret key and “identifying information,” *id.* at [0051]. Thus, the exchange of the secret key and “identifying information” permits the display device to identify the sensor device. Accordingly, the exchange of the “secret key” and “identifying information” corresponds to the claimed “information related to authentication.”

83. Similarly, the time period during which Yarger’s CGM sensor and CGM meter devices exchange the secret key and identifying information via the NFC link, i.e., Step 420 of Fig. 4 (one example of which is depicted in step 804 of Fig. 8), corresponds to the claimed “first interval.”

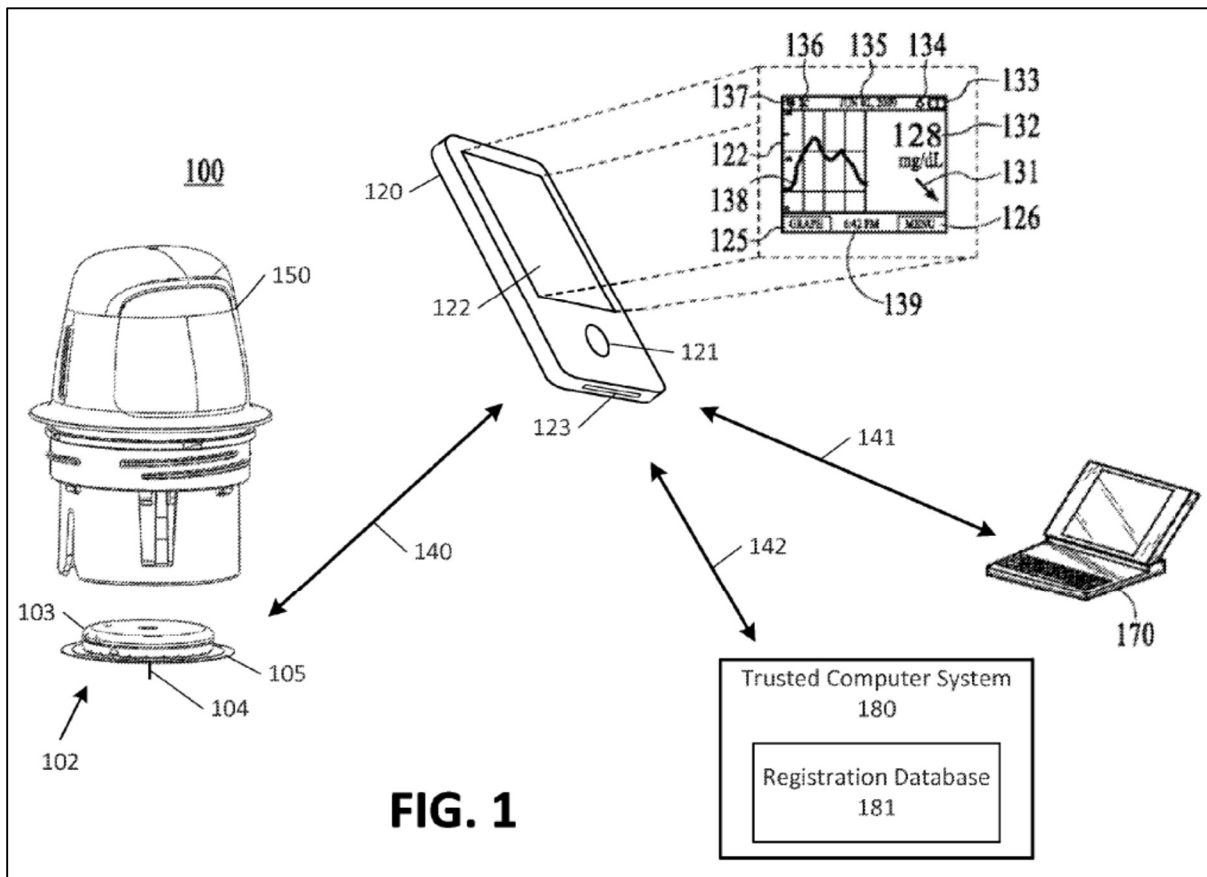
84. Finally, Yarger’s NFC link used to exchange the secret key corresponds to the claimed “first wireless protocol.”

d) 14[c] “performing a determination whether one or more alerts indicative of a medical condition of the host is to be triggered based on the measured analyte data;”

85. Yarger in view of Love suggests this limitation.

86. Yarger discloses that its CGM system is used for monitoring “physiological conditions,” i.e., medical conditions, as part of a “diabetes management system.” Ex. 1005 at Abstract, [0001], [0053]. While Yarger does not

explicitly state that its CGM system determines whether one or more alerts indicative of a medical condition of the host is to be triggered based on the measured analyte data, Love explicitly teaches determining if alarms or alert notifications should be triggered in a CGM system based on measured glucose values received over an encrypted wireless link:



For example, *based on* a determined rate of glucose change, *programmed clinically significant glucose threshold levels (e.g., hyperglycemic and/or hypoglycemic levels)*, and current analyte level derived by an in vivo analyte sensor, an algorithm stored on a computer readable medium of system 100 *can be used to determine the time it will take to reach a clinically significant level and can be used to*

output a notification in advance of reaching the clinically significant level, e.g., 30 minutes before a clinically significant level is anticipated, and/or 20 minutes, and/or 10 minutes, and/or 5 minutes, and/or 3 minutes, and/or 1 minute, and so on, with outputs increasing in intensity or the like.

Ex. 1006 at Fig. 1, [0078]; *see also id.* at [0063], [0070], [0098].

87. In the Yarger-Love combination, the display device in the CGM system that was involved in the exchange of information related to authentication would also determine whether an alert indicative of a medical condition, *i.e.*, predicted low or high glucose levels, should be triggered.

e) 14[d] “triggering at least one alert and providing a notification on the display device when the determination indicates that the at least one alert is to [be] triggered indicative of the medical condition of the host;”

88. Yarger in view of Love suggests this limitation.

89. Love explicitly teaches triggering alarms or alert notifications based on a determination that indicates at least one alert is to be triggered: “In certain embodiments, *reader device 120 can be configured to output alarms, alert notifications, glucose values, etc.*, which may be *visual*, audible, tactile, or any combination thereof.” Ex. 1006 at [0070]; *see also id.* at [0078], [0098].

90. In the Yarger-Love combination, the device in the CGM system that determined whether an alert indicative of a medical condition, *i.e.*, predicted low or

high glucose levels, triggers at least one alert and provides a notification of the alert on the display device.

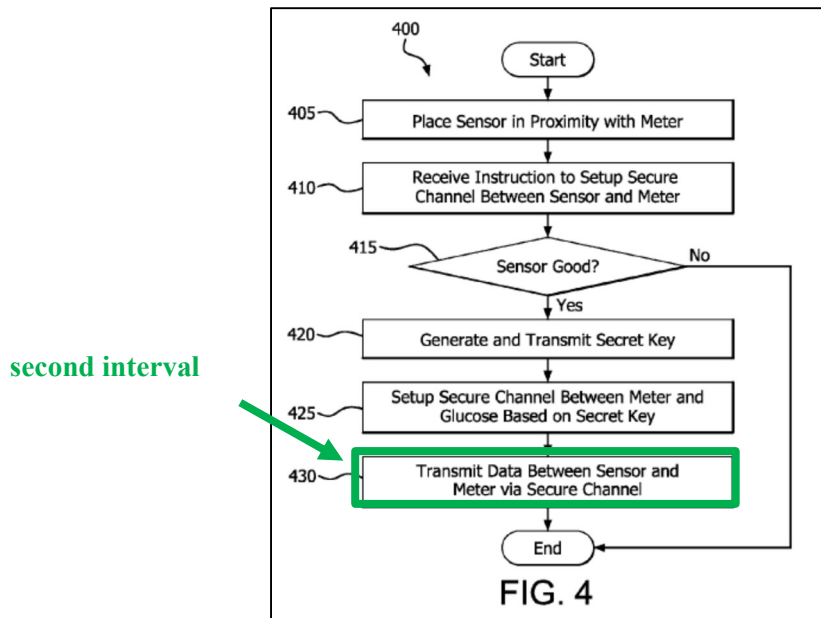
f) 14[e] “during a second interval, bypassing the exchange of information related to authentication by using a second wireless protocol to transmit an encrypted analyte value to the display device,”

91. Yarger discloses this limitation.

92. Yarger discloses bypassing the exchange of the secret key and identifying information (i.e., the information related to authentication) during a second interval by using a second wireless protocol (i.e., Bluetooth, ZigBee, or other wireless protocol) to transmit an encrypted analyte value to a display device:

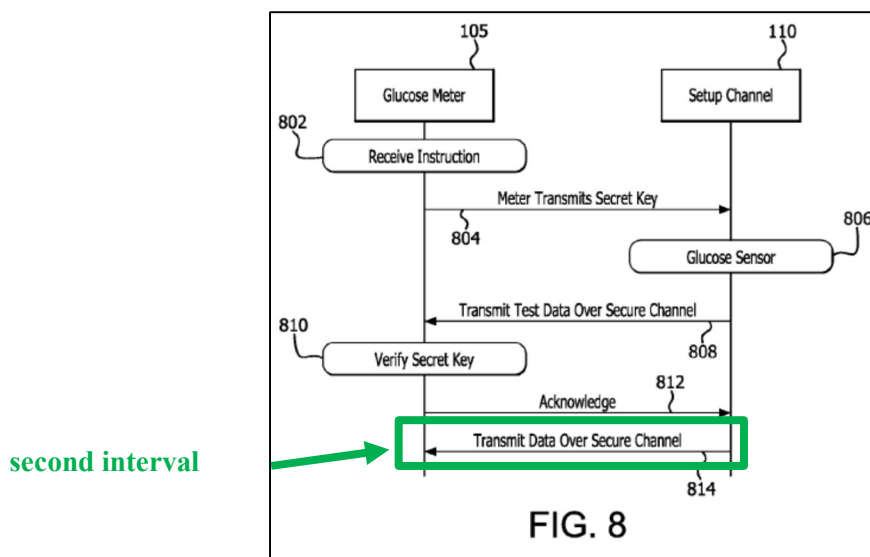
[A]n example glucose meter and an example glucose sensor of the CGM system are placed in proximity to exchange a secret key using a near field wireless link, which is used to ***pair the devices and encrypt data to secure a radio frequency (RF) wireless channel between the sensor and the monitor.***

Ex. 1005 at [0014]; *see also id.* at Abstract. For example, as depicted in Fig. 4, Yarger discloses that the secret key exchanged in the first interval is used to setup a different secure wireless channel between the meter and sensor, with the sensor transmitting encrypted measurement data via the secure wireless channel in step 430 (annotated below):



After both the glucose meter and the glucose sensor have identical secret keys, the glucose sensor and glucose meter *setup a secure wireless channel that is different from the NFC link (e.g., Bluetooth® low power, ZigBee®, a custom wireless link, etc)*. In particular, the glucose meter and glucose sensor *transmit data over the wireless channel that is encrypted using any suitable encryption algorithm* (e.g., advanced encryption standard, data encryption standard, etc.) *using the secret key*, thereby forming a secure wireless link. . . . The receiving device will decrypt the received information using the secret key and verify that the decryption is successful using the error check information.

Id. at Fig. 4 (annotated), [0036]-[0037]. This is also reflected in, for example, Fig. 8, which depicts an embodiment where, once the secret key and identifying information is exchanged during a first interval, data is thereafter transmitted via the secure channel.



Id. at Fig. 8 (annotated), [0047]; *see also id.* at Figs. 5-7.

93. The time period during which Yarger’s CGM sensor transmits encrypted analyte data to the meter via the secure wireless channel, *i.e.*, Step 430 of Fig. 4 (one example of which is depicted in step 814 of Fig. 8), corresponds to the claimed “second interval.” Similarly, Yarger’s secure wireless channel that is different from the NFC link (e.g., Bluetooth® low power, ZigBee®, a custom wireless link, etc.) corresponds to the claimed “second wireless protocol.”

94. Furthermore, Yarger explicitly discloses that the “exchange of information related to authentication” is bypassed during the second interval, because “once transmitted, there generally is no need to exchange the secret key again.” Ex. 1005 at [0035].

g) 14[ff] “wherein the encrypted analyte value has been generated using the information related to authentication, and”

95. Yarger discloses this limitation.

96. Yarger discloses that the secret key exchanged between the sensor and meter (i.e., part of the information related to authentication) is used to generate the encrypted analyte value, “[T]he glucose sensor 110 **uses the secret key to encrypt data** that is transmitted to the glucose meter 105....” Ex. 1005 at [0016]; *see also id.* at [0036] (“the glucose meter and glucose sensor transmit data over the wireless channel that is **encrypted ... using the secret key.**”).

h) 14[g] “wherein the first wireless protocol is different than the second wireless protocol, and”

97. Yarger discloses this limitation.

98. Yarger discloses that the wireless protocol used to exchange the secret key and identifying information (i.e., NFC) is different from the secure RF wireless protocol used for transmission of data (e.g. Bluetooth Low Energy, ZigBee, etc.):

After both the glucose meter and the glucose sensor have identical secret keys, the glucose sensor and glucose meter setup **a secure wireless channel that is different from the NFC link** (e.g., Bluetooth® low power, ZigBee®, a custom wireless link, etc).

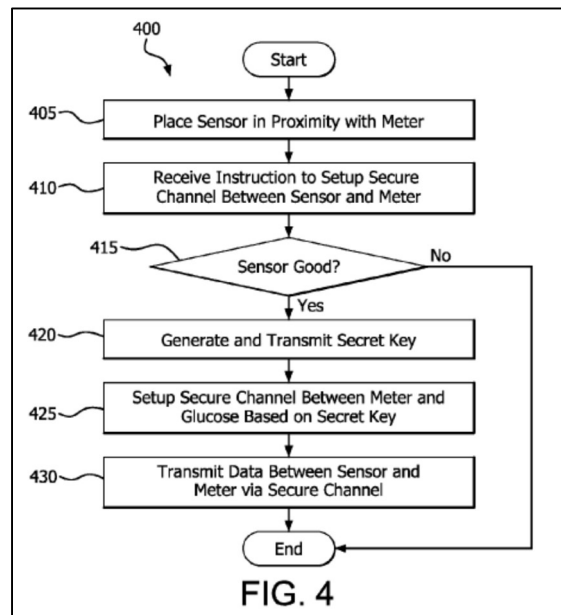
Ex. 1005 at [0036]; *see also id.* at [0016], [0018].

i) 14[h] “neither initiating transmission of analyte values to the display device nor providing a notification on the display device when the information related to

authentication was not exchanged during the first interval.”

99. Yarger and Love both disclose this limitation.

100. Yarger discloses that the CGM sensor does not transmit glucose data to the CGM meter (i.e., display device) if the secret key (i.e., the information related to authentication) was not successfully exchanged during the first interval. For example, Yarger requires the secret key to be exchanged *before* the secure channel can be setup:



After both the glucose meter and the glucose sensor have identical secret keys, the glucose sensor and glucose meter setup a secure wireless channel that is different from the NFC link (e.g., Bluetooth® low power, ZigBee®, a custom wireless link, etc). . . . In another example, the CGM system 100 may verify that the secret key was

successfully received before transmission of glucose measurement data over the secure wireless link.

Ex. 1005 at Fig. 4, [0036]; *see also id.* at Figs. 5-8, [0039]-[0047]. Yarger further discloses with respect to Fig. 8 that if the secret key was not successfully exchanged (determined by verifying and acknowledging test data), then the method will return to the step 804 rather than continue on to the transmission of analyte data:

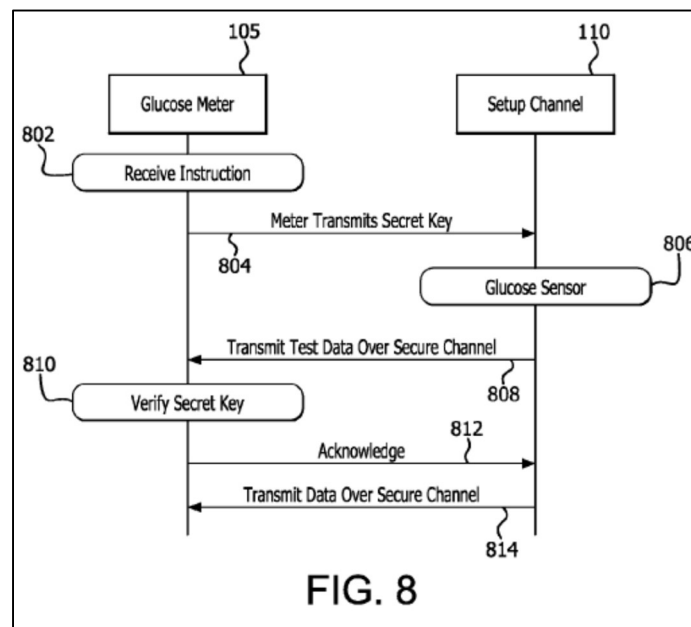


FIG. 8 illustrates another CGM system 100 that verifies successful reception of the secret key. At step 802, the glucose meter 105 receives an instruction to setup a secure wireless link with the glucose sensor 110. In response, the glucose meter 105 generates and transmits a secret key to the glucose sensor 110 at step 804. The glucose sensor 110 stores the secret key at step 806 to initiate setup the secure wireless link. Initially, the glucose sensor 110 transmits test data to the glucose meter 105 at step 808. . . .

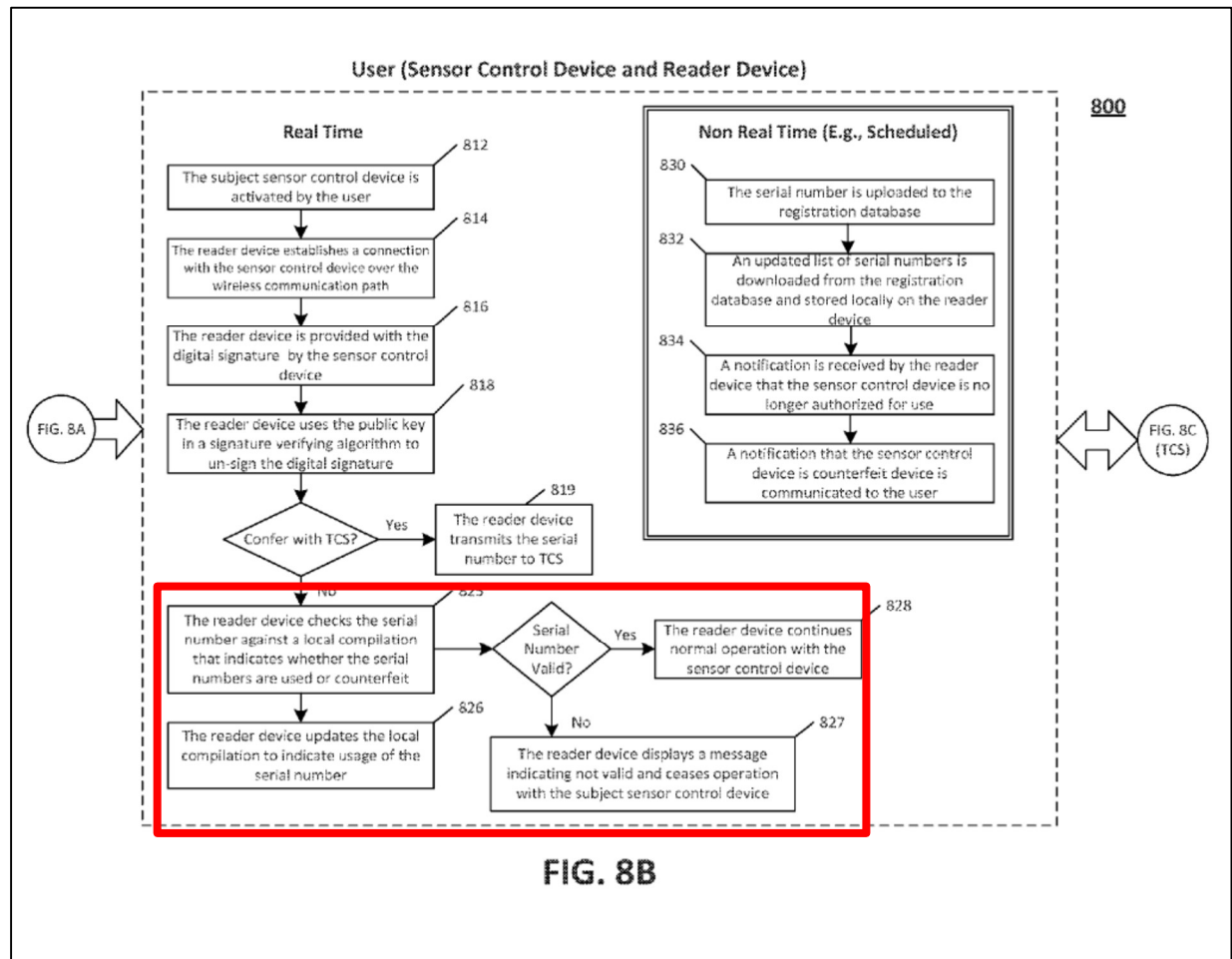
In response to receiving the test data, the glucose meter 105 decrypts the test data and *determines if the test data was successfully received at step 810. . . . In the event that the glucose meter 105 does not verify the secret key at 810, the sequence of communication would return to step 804 until the secret key is successfully determined to be received by the glucose sensor 110.*

Id. at Fig. 8, [0046]-[0047].

101. A POSITA would understand that Yarger’s disclosure describing how the glucose data is not sent over the secure wireless link unless the secret key was first successfully exchanged discloses that the CGM meter (i.e., the display device) would not display any notifications or alerts because the display device must first receive analyte data before making any determinations to display alerts or notifications based on analyte data.

102. As discussed above with respect to claim elements 14[c] and 14[d], Yarger discloses that its CGM system is used for monitoring physiological conditions as part of a “diabetes management system,” with Love explicitly disclosing a CGM system that displays alerts or alarms on a display device in response to determining that the user should be alerted based on measured glucose data received via an encrypted channel. *See, supra*, claims 14[c] and 14[d]. As with Yarger, Love discloses that the sensor control device in its CGM system will not

transmit encrypted analyte data if the exchange of digital signature information (i.e., information related to authentication) was not successful.



At 814, reader device 120 establishes a connection with sensor control device 102 over communication path 140 (see, e.g., FIG. 1). While (or after) establishing the connection, at 816, reader device 120 is provided with digital signature 703 by sensor control device 102. Then, at 818, reader device 120 uses public key 604, which was previously stored in the memory of reader device 120, or was previously retrieved from the manufacturer (e.g., over the internet from trusted computer system 180),

in a signature verifying algorithm to reduce digital signature 703 and obtain the serial number and random number contained therein.

...

If it is determined that the serial number is not valid, either through receipt of the authentication result from trusted computer system 180 or through a local determination at reader device 120, then, at 827 reader device 120 displays a message to the user indicating the same ***and ceases operation with the subject sensor control device 120***.

Ex. 1006 at Fig. 8B (annotated), [0151]-[0155]. Love not only discloses that the information related to authentication is exchanged in a first interval, but also discloses that the information related to authentication must be validated before the sensor and reader device will transmit and display glucose data.

103. Accordingly, Love discloses that the glucose data is not transmitted if the information related to authentication was not successfully exchanged. Because Love discloses that the alarms and alerts shown to the user are based on, *inter alia*, the current analyte levels (*id.* at [0078]), Love's reader device would not display any alerts or notifications to the user based on measured glucose values without first receiving the current glucose levels.

104. Accordingly, a POSITA would have understood that, in the Yarger-Love combination, the sensor device would not initiate transmission of analyte values to the reader, nor would the reader provide a notification on a display, if the

secret key (*i.e.*, information related to authentication) was not exchanged during the first interval.

3. Claim 15

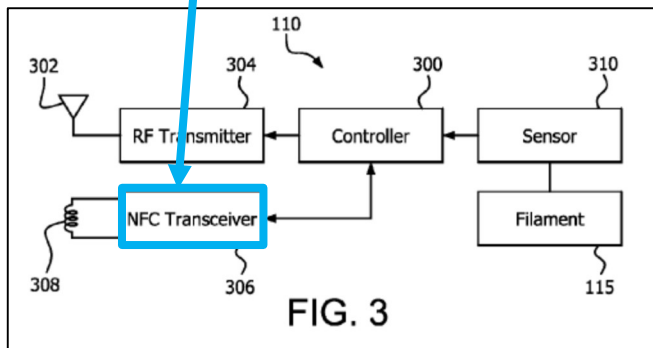
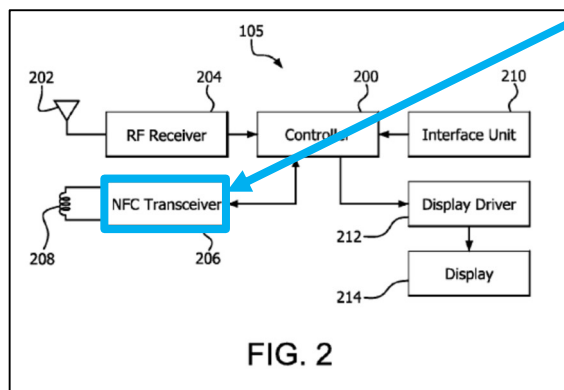
105. Claim 15 depends from claim 14. As explained above the combination of Yarger and Love renders obvious claim 14 as a whole. *See, supra*, claim 14.

- a) 15[a] “wherein the first wireless protocol is selected from the group consisting of: WiFi communication, Near Field Communication (NFC) and Bluetooth Low Energy (BLE) communication; and”

106. Yarger discloses this limitation.

107. Yarger discloses that the first wireless protocol used to perform an exchange of information related to authentication with a display device during a first interval is “near field communication (NFC).” Ex. 1005 at [0018]; *see also id.* at [0023] (discussing pairing via “NFC communication”), [0050]. The NFC transceivers 206, 306 are depicted below in the Fig. 2 (CGM meter 105) and Fig. 3 (CGM sensor 110).

first wireless protocol

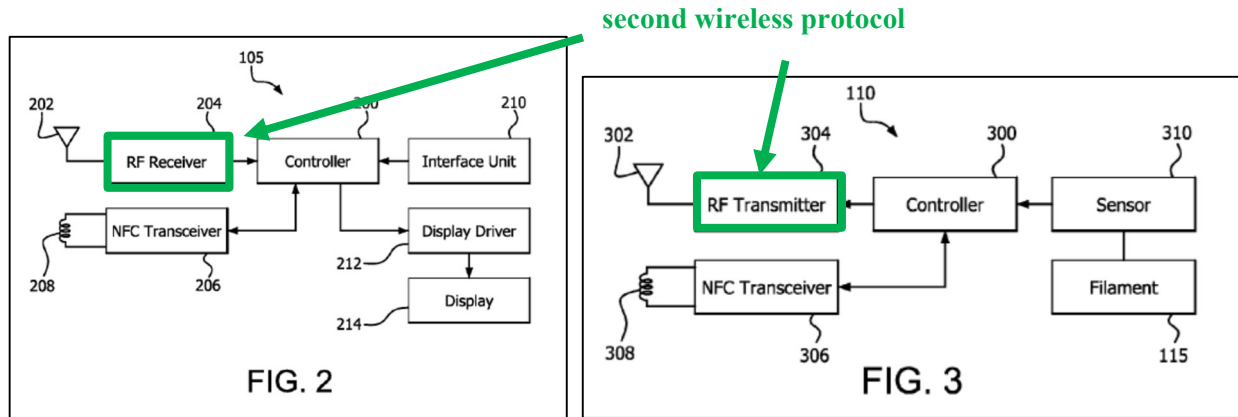


Id. at Figs. 2-3 (annotated), [0026], [0029].

- b) 15[b] “wherein the second wireless protocol is selected from a group consisting of: WiFi communication, NFC and BLE communication.”

108. Yarger discloses this limitation.

109. Yarger discloses that the second wireless protocol used to transmit encrypted analyte data is *different* from the NFC link used to exchange the secret key and can be any number of suitable protocols, including but not limited to ZigBee, Bluetooth low energy (BLE), and 802.11 (Wi-Fi). Ex. 1005 at [0031]; *see also id.* at [0036] (RF link is “different from the NFC link”). The separate RF transceivers 204, 304 are depicted below in Fig. 2 (CGM meter 105) and Fig. 3 (CGM sensor 110).



Id. at Figs. 2-3 (annotated).

4. Claim 16

110. Claim 16 depends from claim 14. As explained above the combination of Yarger and Love renders obvious claim 14 as a whole. *See, supra*, claim 14.

- a) 16[a] “wherein the analyte sensor system is a continuous glucose sensor system and”

111. Yarger discloses this limitation.

112. Yarger discloses that its system is a CGM system: “A physiological condition monitoring system (e.g., *a continuous glucose monitoring system*) includes a physiological condition meter and a physiological condition sensor.” Ex. 1005 at Abstract; *see also id.* at [0001], [0014], [0053].

b) 16[b] “the information related to authentication comprises an application key.”

113. Yarger discloses this limitation.

114. As explained above in claim 14[b], Yarger discloses that during an initial pairing process, the CGM and display devices exchange information related to authentication that includes a secret key, which can comprise a 128 bit “pseudorandom” number, and “identifying information.” *See, supra*, claim 14[b]. As explained above in the ’222 patent at 61:63-64, the claimed application key “may be a random number.” Accordingly, Yarger discloses the information related to authentication comprises an application key.

5. Independent Claim 18

115. The combination of Yarger and Love renders obvious claim 18 as a whole.

a) 18[Pre] “An analyte sensor system configured for wireless communication of analyte data, the analyte sensor system comprising:”

116. Yarger discloses the preamble, to the extent it is limiting.

117. Yarger discloses a system for wireless communication of analyte data.

See, supra, claim 14[Pre].

b) 18[a] “a continuous analyte sensor configured to measure analyte values in a host;”

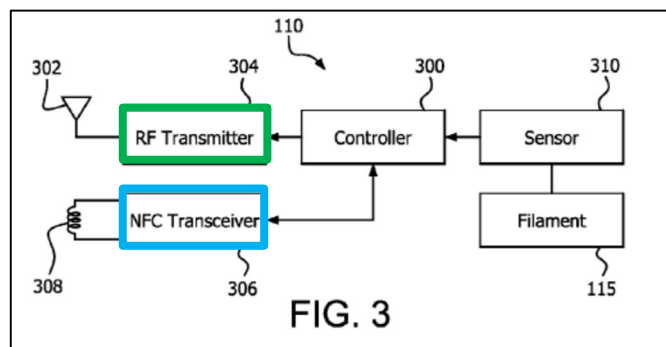
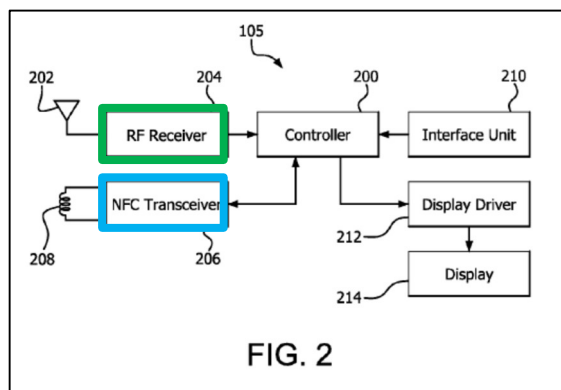
118. Yarger discloses this limitation.

119. *See, supra*, claim 14[a].

c) 18[b] “a transceiver configured to transmit and receive wireless signals; and”

120. Yarger discloses this limitation.

121. Yarger discloses that both the CGM sensor and CGM meter contain multiple transceivers configured to transmit and receive wireless signals, including NFC transceivers (annotated below in blue) for exchanging a secret key and separate RF transceivers for communicating encrypted analyte data (annotated below in green).



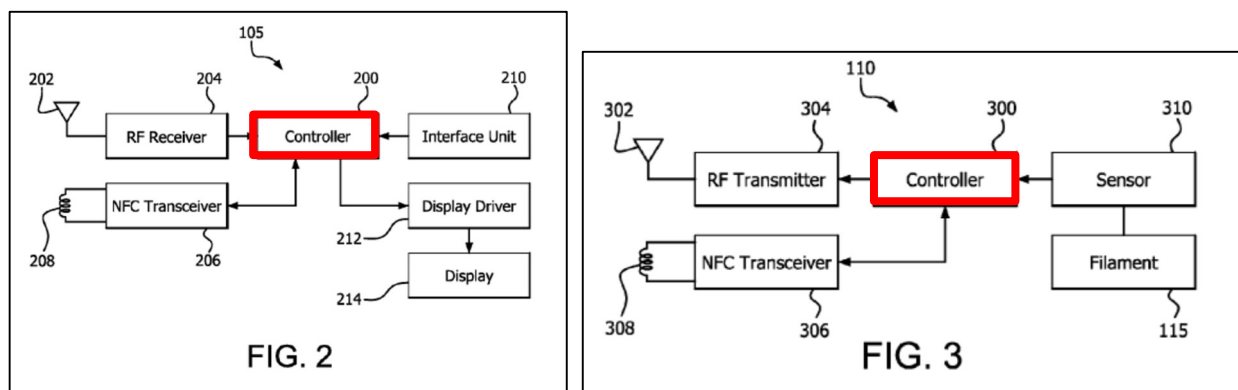
Ex. 1005 at Fig 2 (meter 105, annotated), Fig. 3 (sensor 110, annotated), [0025]-[0031]. While Figures 2 and 3 depict the RF Receiver 204 and RF Transmitter 304,

Yarger discloses that these may also be “RF transceiver[s] for duplex communication.” *Id.* at [0031].

d) 18[c] “a processor operatively coupled to the analyte sensor and the transceiver and configured to cause the analyte sensor system to:”

122. Yarger discloses this limitation.

123. Yarger discloses that both the CGM sensor and CGM meter contain controllers (annotated below in red) operably coupled to the analyte sensor and transceivers, and discloses that these controllers may be, for example, microprocessors.



Ex. 1005 at Fig 2 (meter 105, annotated), Fig. 3 (sensor 110, annotated), [0025] (“controller 200 ... is implemented by any suitable device to control the operation of the glucose meter 105 (e.g., a microcontroller, a *microprocessor*, an application specific integrated circuit, a functional programmable gate array, etc.).”), [0028] (similar for sensor 110); *see generally, id.* at [0025]-[0031].

124. The controller 200 in the CGM meter 105 controls the operation of the CGM meter 105 and is configured to cause the CGM meter 105 to exchange the secret key with the sensor 110, receive encrypted analyte data from sensor 110, and to control the display. *Id.* at [0025]-[0027]. Similarly, the controller 300 in the CGM sensor 110 controls the operation of the sensor and is configured to cause the CGM sensor to exchange the secret key with the CGM meter 105, receive measurements from the glucose sensor, and transmit encrypted analyte data. *Id.* at [0028]-[0030]. A POSITA would thus understand that the controllers 200, 300 in Yarger are configured to cause the analyte sensor system to perform the functions discussed below in claim elements 18[d]-18[j].

e) 18[d] “during a first interval, establish a first connection between the analyte sensor system and a display device;”

125. Yarger discloses this limitation.

126. As explained above in claim 14[b], Yarger discloses using a first wireless protocol (i.e., NFC) to perform an exchange of information related to authentication with a glucose meter (i.e., a display device) during a first interval. *See, supra*, claim 14[b]. The NFC connection corresponds to the “first connection.”

f) 18[e] “during the first connection, exchange information related to authentication between the analyte sensor system and the display device;”

127. Yarger discloses this limitation.

128. As explained above in claim 14[b], Yarger discloses using a first wireless protocol (i.e., NFC) to exchange a secret key (i.e., the claimed information related to authentication) between a glucose sensor and a glucose meter with a display to pair the glucose sensor and glucose meter. *See, supra*, claim 14[b].

g) 18[ff] “perform a first determination whether authentication was performed during the first interval;”

129. Yarger and Love both disclose this limitation.

130. As explained above in claim 14[h], Yarger discloses a determination of whether the secret key was successfully exchanged during the first interval based on exchange of test data using the secret key and Love discloses that the sensor control device in its CGM system will not transmit encrypted analyte data if the exchange of digital signature information (i.e., information related to authentication) was not successful. *See, supra*, claim 14[h]. Yarger’s determination of whether the secret key was successfully exchanged corresponds to the “first determination whether authentication was performed during the first interval.” Love’s determination of whether the digital signature information was successfully exchanged corresponds to the “first determination whether authentication was performed during the first interval.”

h) 18[g] “perform a second determination whether one or more alerts indicative of a medical condition of the host is to be triggered based on the measured analyte data;”

131. Yarger in view of Love suggests this limitation.

132. *See, supra*, claim 14[c].

- i) 18[h] “trigger at least one alert and provide a notification on the display device when the second determination indicates that the at least one alert is to triggered indicative of the medical condition of the host; and”

133. Yarger in view of Love suggests this limitation.

134. *See, supra*, claim 14[d].

- j) 18[i] “during a second interval, transmit an encrypted analyte value to the display device, when the first determination indicates that the authentication was performed during the first interval, and”

135. Yarger discloses this limitation.

136. *See, supra*, claim 14[e].

- k) 18[j] “neither initiate transmission of analyte values to the display device if nor provide a notification on the display device when the first determination indicates that the authentication was not performed during the first interval.”

137. Yarger and Love both disclose this limitation.

138. *See, supra*, claim 14[h].

6. Claim 19

139. Claim 19 depends from claim 18. As explained above the combination of Yarger and Love renders obvious claim 18 as a whole. *See, supra*, claim 18.

- a) 19[a] “wherein the processor is further configured to cause the analyte sensor system to: during the second

interval, establish a second connection between the analyte sensor system and the display device; and”

140. Yarger discloses this limitation.

141. As explained above in claim 14[e], Yarger discloses using a second wireless protocol (e.g., BLE, Wi-Fi, ZigBee) to communicate the encrypted analyte data during a second interval. *See, supra*, claim 14[e]. The RF connection (whether BLE, Wi-Fi, ZigBee, or other protocol) corresponds to the “second connection.”

b) 19[b] “during the second connection, bypass the exchange of the information related to authentication.”

142. Yarger discloses this limitation.

143. *See, supra*, claim 14[e].

7. Claim 20

144. Claim 20 depends from claim 19. As explained above the combination of Yarger and Love renders obvious claim 19 as a whole. *See, supra*, claim 19.

a) 20[a] “wherein the analyte sensor system is a continuous glucose sensor system, and”

145. Yarger discloses this limitation.

146. *See, supra*, claim 16[a].

b) 20[b] “the information related to authentication comprises an application key”

147. Yarger discloses this limitation.

148. *See, supra*, claim 16[b].

- c) 20[c] “wherein the processor is further configured to cause the analyte sensor system to use the application key to encrypt an analyte value including a glucose value measured by the continuous analyte sensor to generate the encrypted analyte value including an encrypted glucose value, and”

149. Yarger discloses this limitation.

150. Yarger discloses that the secret key exchanged between the sensor and meter (i.e., the application key) is used to encrypt the analyte data for transmission. *See, supra*, claim 14[f].

- d) 20[d] “wherein the use of the application key allows the analyte sensor system to bypass the exchange.”

151. Yarger discloses this limitation.

152. *See, supra*, claim 14[e].

B. Ground 2: The Challenged Claims Are Rendered Obvious By Hernandez-Rosas In View Of Chivallier

153. Hernandez-Rosas discloses (1) a wireless CGM system that exchanges information related to authentication prior to transmission of encrypted analyte values and (2) that the display device can display notifications to a user based on the received analyte levels. Chivallier discloses exchanging the information related to authentication via a different wireless protocol from the protocol used to communicate the encrypted analyte values. The combination of Hernandez-Rosas and Chivallier renders the challenged claims obvious, as explained in more detail below.

1. A POSITA Would Have Been Motivated to Combine Hernandez-Rosas and Chivallier and Would Have Reasonably Expected Success in Doing So.

154. Hernandez-Rosas describes a CGM system with secure communication of glucose data between a sensor device and a display device (e.g. a mobile device), including an authentication procedure to authenticate the sensor device and mobile device. Ex. 1007 at Abstract. Hernandez-Rosas discloses that authentication is “required for communication between the sensor electronics module and the display device.” *Id.* at [0119]. Hernandez-Rosas further discloses that once authentication has occurred, the sensor device and display device may exchange information relating to encryption. *Id.* at [0150].

155. A POSITA would have understood that a successful authentication and encryption scheme would prevent an eavesdropper or man-in-the-middle from intercept and determine the encryption key, otherwise an unauthorized device might be able to mimic the authentication steps. A POSITA would thus have understood the importance of ensuring that the wireless link used to transmit the authentication information and encryption information is secure from eavesdropping.

156. Chivallier discloses a method for data transmission between a sensor device and a mobile device with an authentication step for establishing a secure wireless communication link. Ex. 1008 at Abstract, [0004]-[0005]. Chivallier further discloses that to initiate the authentication process, a mobile phone is brought into

“close proximity” with a sensor device, and a private key is transmitted from the sensor device to the mobile device via an NFC link. *Id.* at [0017]-[0020], [0028]. Chivallier’s mobile device then uses a public key corresponding to the sensor’s private key to recognize and authenticate the sensor. *Id.* at [0029]. After authentication has succeeded, Chivallier’s sensor and mobile device communicate via a different communication protocol, such as Bluetooth, ZigBee, ultra-wide band or other appropriate protocol, with the sensor data being encrypted using the private key transmitted via the short range NFC link. *Id.* at [0016], [0030]-[0031].

157. As I explained in the Technology Background above, a POSITA would have understood that the range of an NFC communication is on the order of a few centimeters. Therefore, a POSITA would have understood that the use of the NFC link in Chivallier to exchange the private key is effective to prevent eavesdroppers from intercepting the private key used to encrypt the data sent on a different wireless link.

158. Hernandez-Rosas and Chivallier both disclose CGM systems with secure wireless communication with a display device and thus are both in the same field as the ’222 Patent.

159. It would have been obvious to incorporate Chivallier’s use of NFC to exchange the initial authentication and pairing information into CGM system of

Hernandez-Rosas so that the initial authentication and pairing process in Hernandez-Rosas would be more secure.

160. A POSITA would have been motivated to adopt Chivallier's use of the short-range NFC link to exchange the initial pairing and authentication information in the CGM system of Hernandez-Rosas in order to achieve Hernandez-Rosas's stated goal of providing for authentication in order to prevent the risk of eavesdropping that can occur with other longer-range wireless links.

161. Combining Hernandez-Rosas and Chivallier would have been combining prior art elements (Hernandez-Rosas's CGM system with encrypted wireless communication between a glucose sensor with Chivallier's use of a different, shorter range wireless protocol for the initial authentication and pairing steps) according to known methods to yield predictable results (i.e., a CGM with a secure authentication and pairing step via NFC and with longer range wireless communication of analyte values once paired). Combining Hernandez-Rosas and Chivallier would also have been a use of a known technique (i.e., adding the NFC tag and reader of Chivallier) to improve similar devices in the same way (i.e., utilizing a CGM reader device with wireless transceiver to perform an initial authentication and pair and later transmit encrypted analyte data).

162. A POSITA would have a reasonable expectation of success of adopting the NFC link of Chivallier for the initial exchange of authentication information in

addition to a separate wireless link in the CGM system of Hernandez-Rosas because NFC transmitters and receivers were well-known as of the effective filing date of the '222 patent and it would have been within the skill of a POSITA to incorporate these transceivers to the CGM system of Hernandez-Rosas with its existing wireless transceivers. *See, e.g.,* Ex. 1008 at Fig. 2 (CGM system with NFC transmitter/receivers and separate discrete wireless connectivity modules); Ex. 1005 at Figs. 2, 3 (CGM system with separate NFC transmitter/receiver and RF transmitter/receiver).

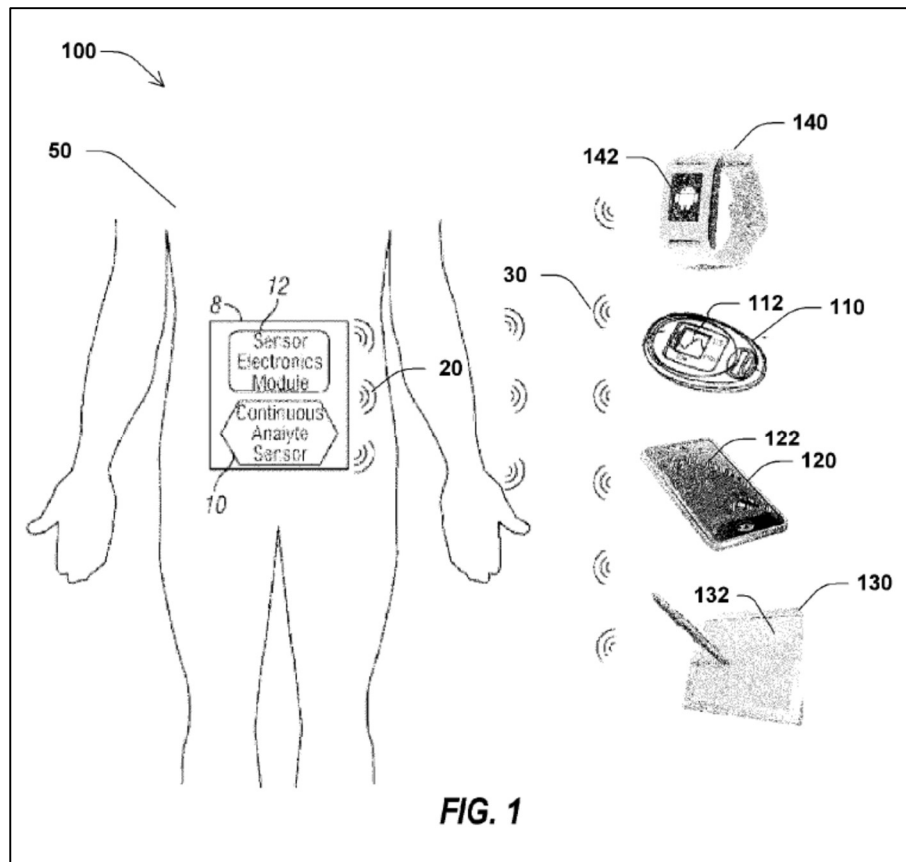
2. Independent Claim 14

163. The combination of Hernandez-Rosas and Chivallier renders obvious claim 14 as a whole.

a) 14[Pre] “A method for wireless communication of analyte data, the method comprising”

164. Hernandez-Rosas discloses the preamble, to the extent it is limiting.

165. Hernandez-Rosas discloses a method for wireless communication of analyte data.



In a first aspect, a method for a *wireless data communication between an analyte sensor system and a mobile device capable of wirelessly receiving analyte values* from the analyte sensor system is provided.

Ex. 1007 at Fig. 1, [0007]; *see also id.* at Abstract, [0124]-[0127].

Wireless communication protocols may be used to transmit and receive data between the sensor system 8 and the display device 110, 120, 130, 140.

Id. at [0140].

b) 14[a] “measuring analyte values in a host using a continuous analyte sensor of an analyte sensor system;”

166. Hernandez-Rosas discloses this limitation.

167. Hernandez-Rosas discloses a CGM system that measures analyte values using a “continuous analyte sensor.”

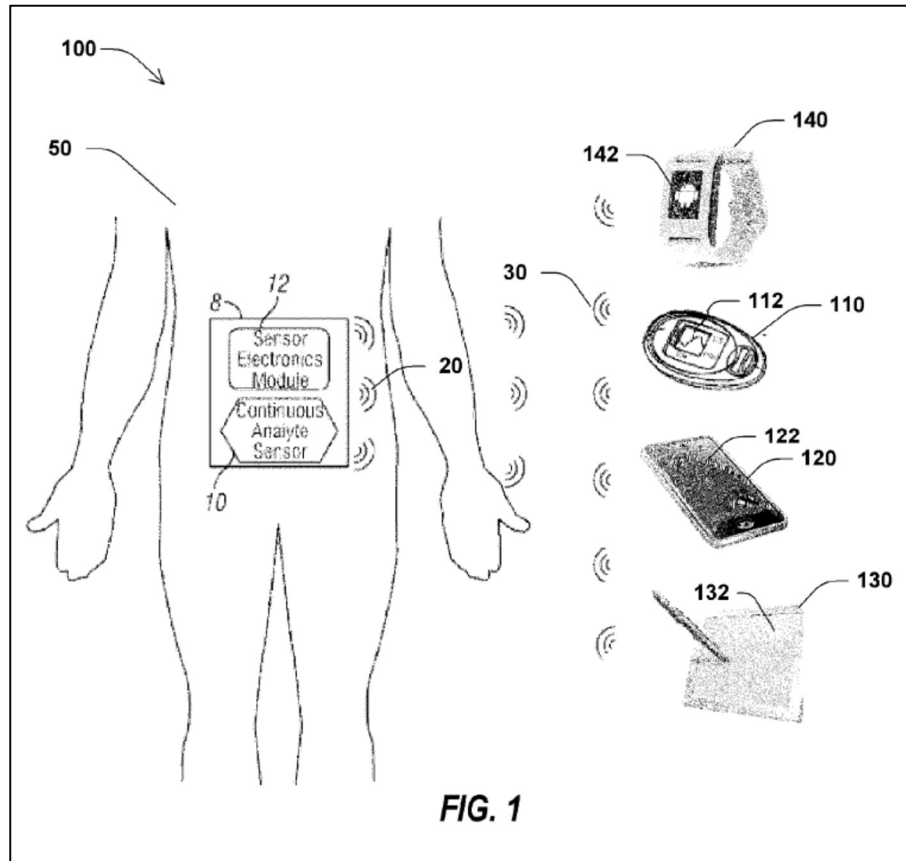


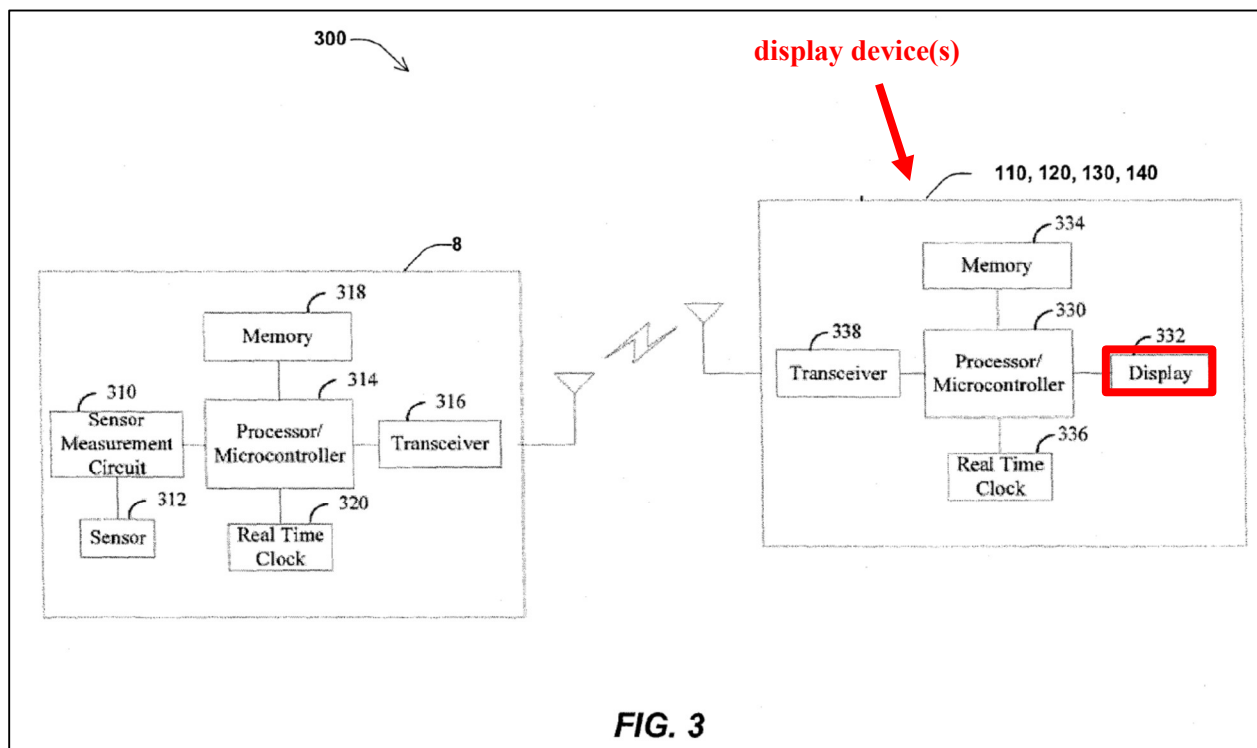
FIG. 1 is a diagram depicting an *exemplary continuous analyte monitoring system 100* including an analyte sensor system 8 and a plurality of display devices 110, 120, 130, 140 according to certain aspects of the present disclosure. The analyte sensor system 8 includes a sensor electronics module 12 and *a continuous analyte sensor 10* associated with the sensor electronics module 12.

Ex. 1007 at Fig. 1, [0124]; *see also id.* at [0104], [0125], [0130] (“analyte sensor 10 of FIG. 1 comprises *a continuous glucose sensor*”), Fig. 3.

c) 14[b] “during a first interval, using a first wireless protocol to perform an exchange of information related to authentication with a display device;”

168. Hernandez-Rosas discloses this limitation.

169. Hernandez-Rosas discloses performing an exchange of information related to authentication via a challenge-and-response protocol between a CGM sensor and a display device during a first interval:

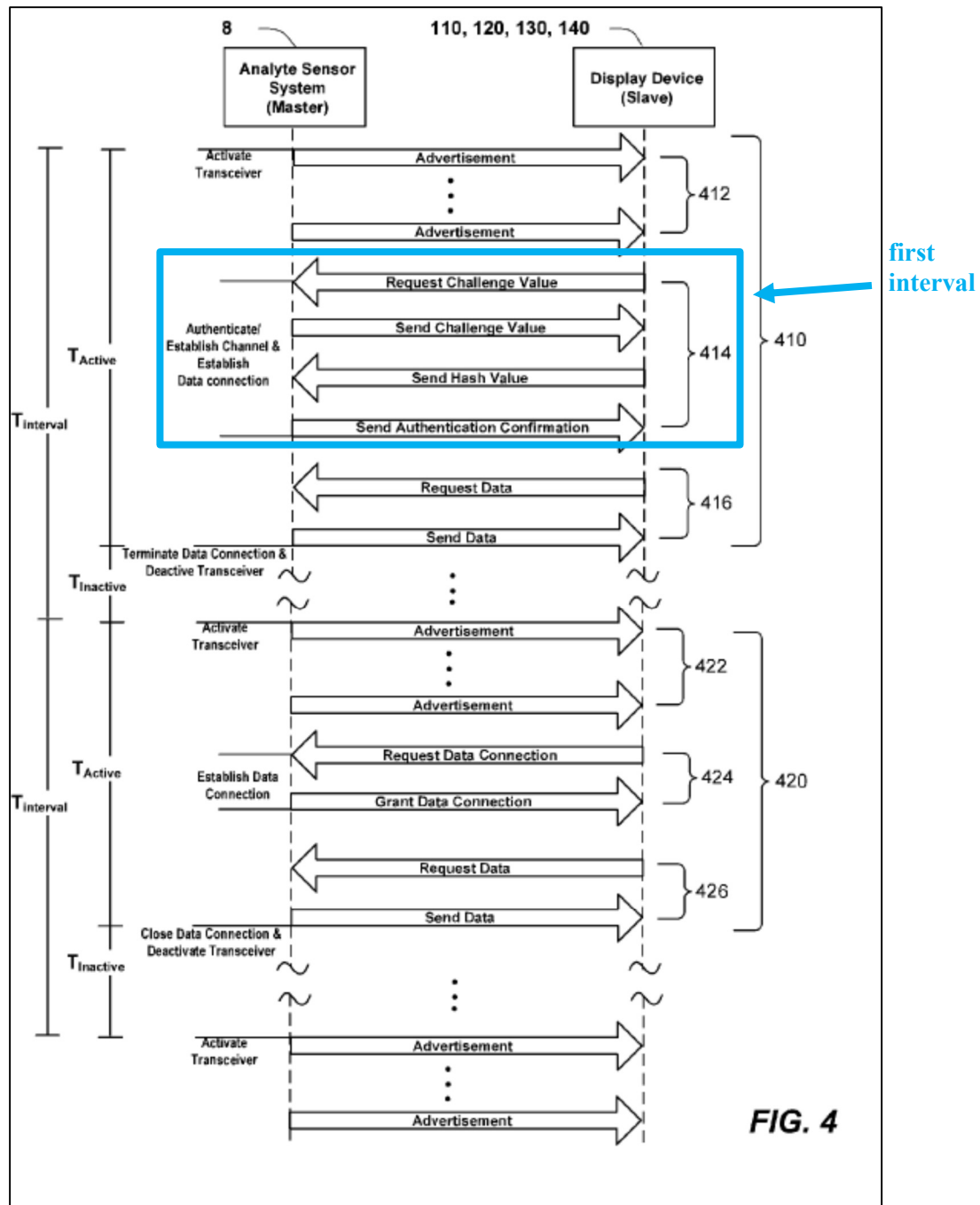


Ex. 1007 at Fig. 3 (annotated).

In certain embodiments, one or more *display devices* comprise built-in authentication mechanisms, wherein authentication is required for communication between the sensor electronics module and the display device. In some embodiments, to authenticate the data communication between the sensor electronics module and display devices, *a*

challenge-response protocol, such as a password authentication is provided, where the challenge is a request for the password and the valid response is the correct password, such that pairing of the sensor electronics module with the display devices can be accomplished by the user and/or manufacturer via the password.

Id. at [0119], *see also id.* at [0144], Fig. 4, [0147]-[0150]. For example, Hernandez-Rosas discloses in Figure 4 a first wireless communication session 410 (annotated in blue) involving an exchange of information related to authentication during a first data connection process 414:

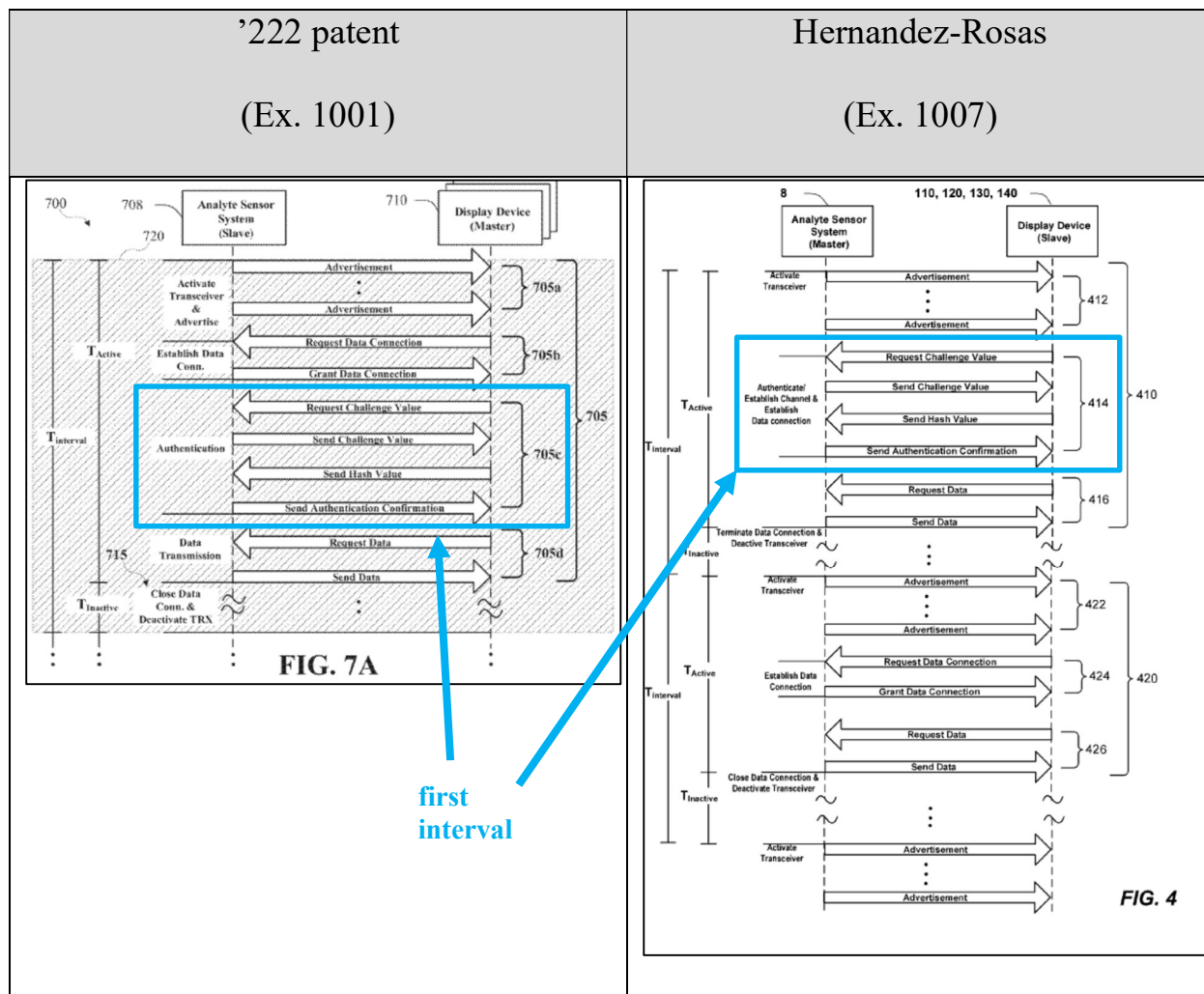


After an advertisement signal is successfully received by a display device 110, 120, 130, 140, the display device and the analyte sensor system 8 engage in a first data connection process 414. ***During the first data connection process 414***, the display device requests a challenge value from the analyte sensor system 8 and the analyte sensor system 8

sends the change value to the display device in response. Upon receiving the challenge value, ***the display device calculates a hash value based on the challenge value and the identification information*** associated with the analyte sensor system 8 and/or the transceiver 316 and sends the hash value to the transceiver 316. The transceiver 316 receives the hash value from the display device 110, 120, 130, 140, decodes the identification information from the hash value, and ***verifies that the received identification information matches identification information associated with the sensor system 8 and/or transceiver 316*** previously stored in the memory 318 of the analyte sensor system 8, such as during manufacturing of the sensor system 8. ***Upon verification, the transceiver 316 sends a signal confirming a successful authentication*** to the display device 110, 120, 130, 140. Once authenticated, the analyte sensor system 8 and display device 110, 120, 130, 140 may exchange information to determine how data will be exchanged (e.g., a specific frequency, time slot assignment, encryption, etc.).

Ex. 1007 at Fig. 4 (annotated), [0150]; *see also id.* at [0148].

170. Notably, the “first data connection process 414” in Fig. 4 from Hernandez-Rosas (assigned to DexCom) is nearly identical to “authentication procedure 705c” of Fig. 7A in the ’222 patent, as depicted below:

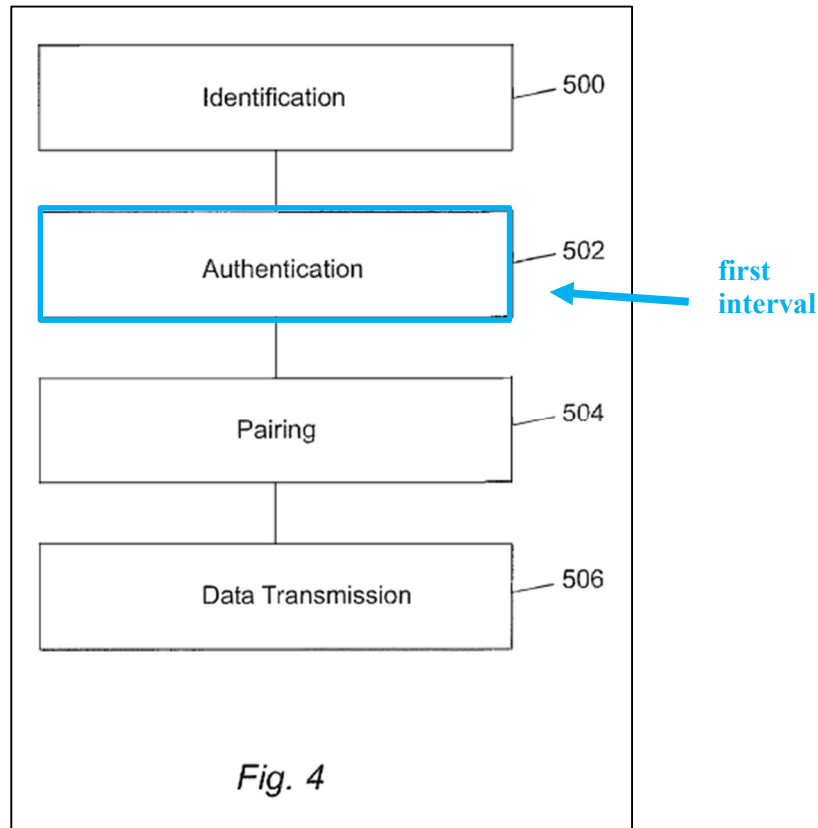


Compare Ex. 1001 at Fig. 7A (annotated), 60:42-61:15, with Ex. 1007 at Fig. 4 (annotated), [0150]. Accordingly, the first data connection process 414 in Hernandez-Rosas corresponds to the claimed “first interval” in the ’222 patent.

171. Hernandez-Rosas further discloses that the wireless data communication utilizes any of “Wi-Fi, Bluetooth, and Bluetooth low energy (BLE)” protocols. Ex. 1007 at [0160]; *see also id.* at [0016], [0052]. Accordingly, the Wi-

Fi, Bluetooth, or Bluetooth Low Energy protocols correspond to the claimed “first wireless protocol.”

Likewise, Chivallier discloses an authentication process 502 that occurs in a first interval before a pairing process 504:



The authentication process uses a dual key handling secure process with a private and public key encryption through the well-known RSA encryption algorithm with digital signatures and certificates. The authentication process can occur between the sensor module 202 and the mobile device 300. The process may use the sensor private key stored in the SE 209 of the sensor module 202 and the public key stored in the SE 309 of the NFC tag reader 308 to enable authentication. ***The public key in the SE 309 is used to recognize and authenticate the***

private key of sensor 202 by means of the certificates. At the end of the mutual authentication process, *if there is a matching between the private stored key in the NEC [sic] tag 209 of the sensor module 202 and the public stored key in the NFC tag reader 308, the sensor module 202 is fully authenticated* as being the sensor module 202 compatible with the mobile device 300.

Ex. 1008 at Fig. 4 (annotated), [0029].

d) 14[c] “performing a determination whether one or more alerts indicative of a medical condition of the host is to be triggered based on the measured analyte data;”

172. Hernandez-Rosas discloses this limitation.

173. Hernandez-Rosas discloses that the system makes a determination of whether to trigger one or more alerts indicative of a medical condition of a host (e.g. hypoglycemia) based on the measured analyte data.

In certain embodiments, one or more alerts are associated with a sensor electronics module. For example, *each alert may include one or more alert conditions that indicate when the respective alert has been triggered*. For example, a hypoglycemic alert may include alert conditions indicating a minimum glucose level.

Ex. 1007 at [0107]; *see also* [0108]-[0109].

In some embodiments, dynamic and intelligent estimation *determines a possibility of the patient avoiding clinical risk, based on the analyte concentration*, the rate of change, and other aspects of the dynamic and

intelligent estimative algorithms. *If there is minimal or no possibility of avoiding the clinical risk, a clinical risk alert will be triggered.*

Id. at [0110]; *see also* [0112].

- e) 14[d] “triggering at least one alert and providing a notification on the display device when the determination indicates that the at least one alert is to [be] triggered indicative of the medical condition of the host;”

174. Hernandez-Rosas discloses this limitation.

175. Hernandez-Rosas discloses triggering alarms or alert notifications on the display device based on a determination that indicates at least one alert is to be triggered:

In certain embodiments, each of the alerts is associated with one or more *actions that are to be performed in response to triggering of the alert*. Alert actions may include, for example, *activating an alarm, such as displaying information on a display of the sensor electronics module* or activating an audible or vibratory alarm coupled to the sensor electronics module, and/or transmitting data to one or more display devices external to the sensor electronics module.

Ex. 1007 at [0108]; *see also id.* at [0107], [0109].

In some embodiments, *the sensor electronics module is configured to provide one or a plurality of different alarms via the sensor electronics module* and/or via transmission of a data package indicating an alarm should be initiated by one or a plurality of display devices (e.g., sequentially and/or simultaneously). . . . In some embodiments, the sensor electronics module determines which of the one or more alarms

to trigger based on one or more alerts that are triggered. *For example, when an alert trigger indicates severe hypoglycemia, the sensor electronics module can perform multiple actions, such as activating an alarm on the sensor electronics module*, transmitting a data package to a monitoring device indicating activation of an alarm on the display, and transmitting a data package as a text message to a care provider.

Ex. 1007 at [0112].

f) 14[e] “during a second interval, bypassing the exchange of information related to authentication by using a second wireless protocol to transmit an encrypted analyte value to the display device,”

176. Hernandez-Rosas discloses this limitation.

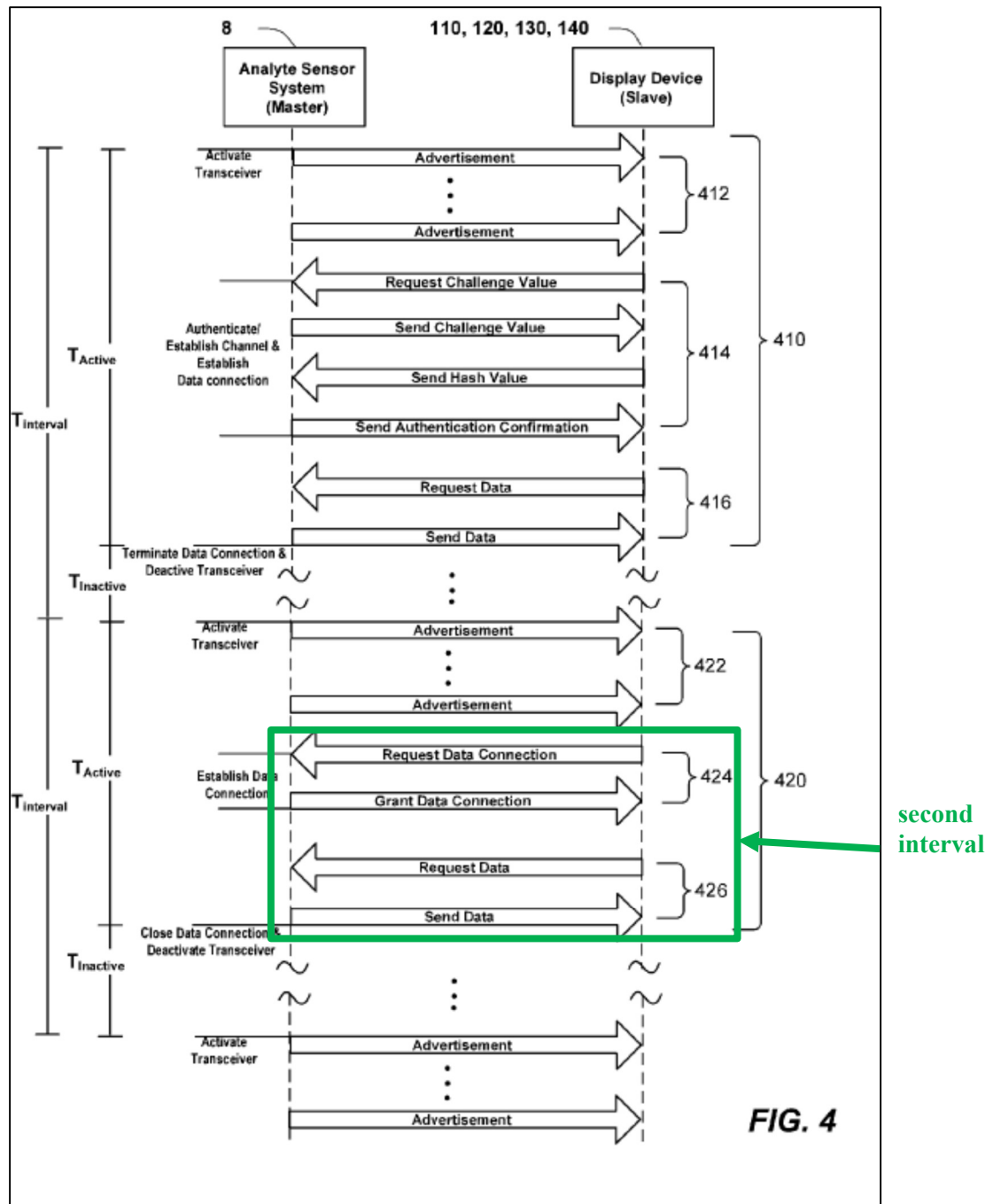
177. Hernandez-Rosas discloses bypassing the exchange of information related to authentication in order to wirelessly transmit encrypted analyte values to a display device during a second interval.

As will be further described below, there may be a process for initially establishing communication between a display device 110, 120, 130, 140 and the sensor electronics module when it is first used or re-activated (e.g., the battery is replaced). *Once the display device 110, 120, 130, 140 and sensor electronics module have established communication, the display device 110, 120, 130, 140 and sensor electronics module may periodically and/or continuously be in communication* over the life of several sensors 312 until, for example,

the battery needs to be replaced. Each time a sensor 312 is replaced, a new sensor session may be established.

Ex. 1007 at [0144]; *see also id.* at [0147]-[0152].

178. For example, Hernandez-Rosas discloses in Fig. 4 a second wireless communication session 420 involving a second data connection process 424 and second data communication process 426 that bypasses the exchange of authentication information in first data connection process 414 of first wireless communication session 410:

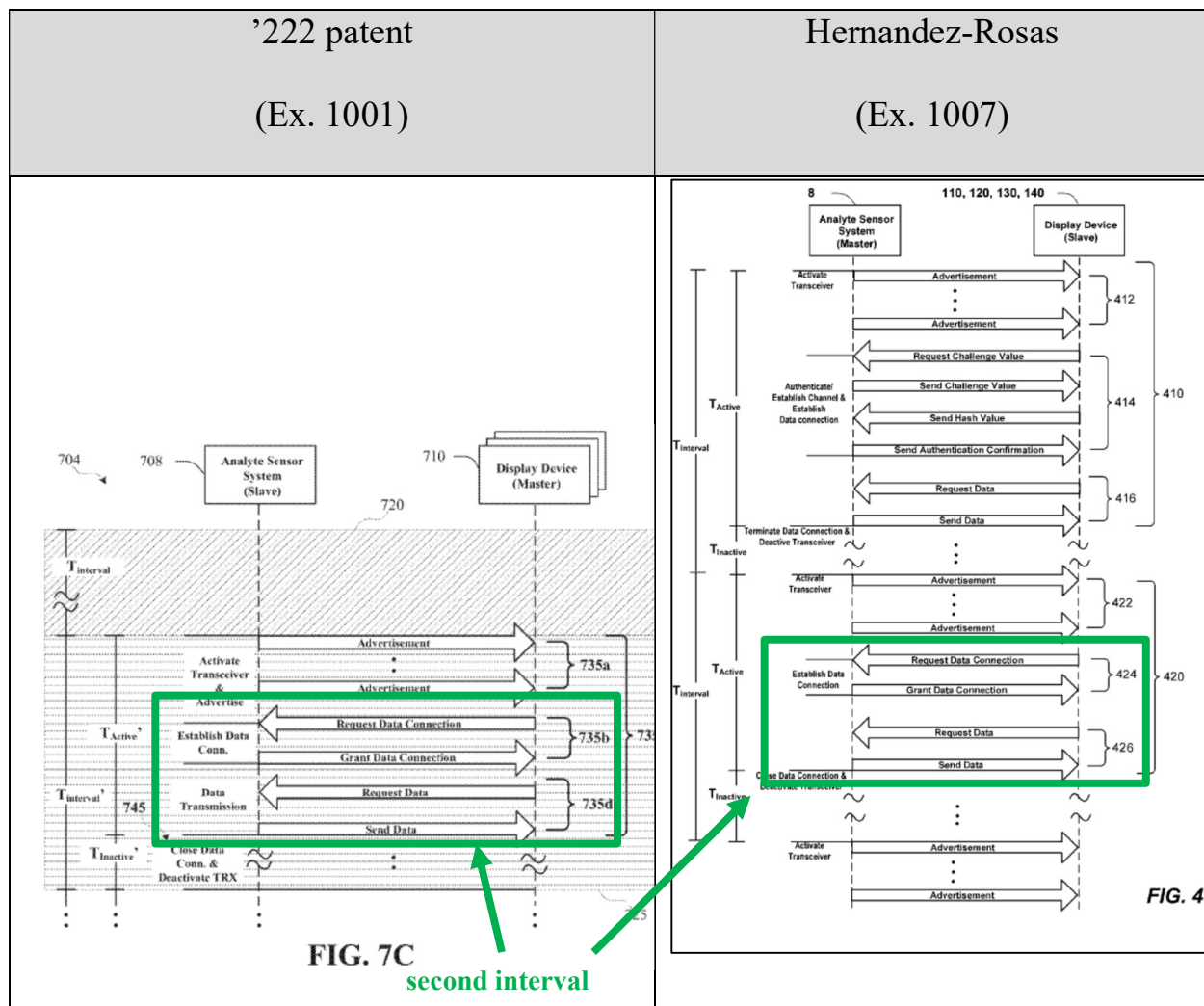


After an inactive time or period $T_{Inactive}$, a second wireless communication session 420 starts when the transceiver 316 (and the transceiver 338) powers up again, begins transmitting a second series of advertisement signals 422, engages in *a second data connection process 424 and a second data communication process 426* with the

transceiver 338 of the display device 110, 120, 130, 140 as shown in FIG. 4. Unlike the first data connection process 414, however, the *second data connection process 424 does not involve an authentication because the analyte sensor system 8 and the display device 110, 120, 130, 140 have been successfully paired or bonded during the first wireless communication session 410 as described above.*

Ex. 1007 at Fig. 4 (annotated), [0152].

179. As with the first interval, the “second data connection process 424” and “second data communication process 426” portion of second communication session 420 in Fig. 4 from Hernandez-Rosas (assigned to DexCom) is nearly identical to second connection operation 735b and data transmission operation 735d of Fig. 7C in the '222 patent, as depicted below:



Compare Ex. 1001 at Fig. 7C (annotated) , 64:59-66, with Ex. 1007 at Fig. 4 (annotated), [0152]. Accordingly, the second data connection process 424 and second data communication process 426 in Hernandez-Rosas corresponds to the claimed “second interval.”

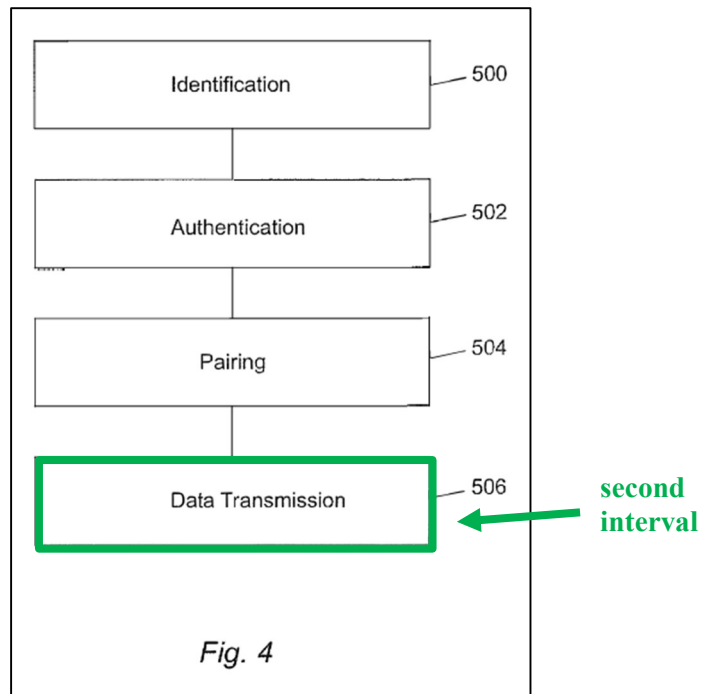
180. Hernandez-Rosas further discloses that the wireless data communication utilizes any of “WiFi, Bluetooth and Bluetooth low energy (BLE)” protocols. Ex. 1007 at [0160]; *see also id.* at [0016], [0052]. Accordingly, the Wi-

Fi, Bluetooth, or Bluetooth Low Energy protocols correspond to the claimed “second wireless protocol.”

181. To the extent this claim limitation requires the first and second wireless protocols to be different protocols, Hernandez-Rosas in view of Chivallier suggests this limitation.

182. Hernandez-Rosas does not explicitly state that the wireless protocol used during the first interval and second interval are different protocols, although it allows for such situations (e.g., Wi-Fi and Bluetooth). However, Chivallier explicitly discloses this and the combination of Hernandez-Rosas and Chivallier render obvious the claim as a whole. *See, infra*, claim element 14[g].

183. Furthermore, Hernandez-Rosas discloses that the wireless data communication in the second interval may be encrypted. *Id.* at [0150] (explaining that “the analyte sensor system 8 and display device 110, 120, 130, 140 may exchange information to determine how data will be exchanged (e.g., a specific frequency, time slot assignment, encryption, etc.)”). Chivallier also discloses encrypted data communication in a second data transmission interval 506 after authentication 502:



184. Ex. 1008 at Fig. 4 (annotated). Chivallier explains that after “the identification step 500, the authentication step 502 and the pairing step 504 have been completed successfully, the transmission of stored data can occur as indicated in step 506. The stored data are encrypted using the private key stored in the SE 210 of the sensor module 202.” *Id.* at [0031].

185. In the Hernandez-Rosas-Chivallier combination, the CGM sensor and display device use a first wireless protocol to exchange the information related to authentication and subsequently use a different, second wireless protocol to transmit encrypted analyte data (*e.g.*, the first wireless protocol is NFC while the second wireless protocol is Bluetooth).

g) 14[ff] “wherein the encrypted analyte value has been generated using the information related to authentication, and”

186. Hernandez-Rosas discloses this limitation.

187. Hernandez-Rosas further discloses that the wireless data communication, including the communication of the analyte values, may be encrypted. Ex. 1007 at [0150].

188. While Hernandez-Rosas does not explicitly state that the analyte values transmitted in the data connections of Fig. 4 are encrypted using the information related to authentication, Hernandez-Rosas discloses, with respect to Fig. 11, that the sensor can transmit “encoded” analyte values such that decoding the encoded analyte value uses “a key or code that can be generated by the use of the identification information associated with the analyte sensor system 1010.” *Id.* at [0200]. A POSITA would understand that this disclosure is referring to the encryption of the analyte values because of the reference to using the “key” to decode the analyte values. Thus, Hernandez-Rosas suggests encrypting the analyte values using the information related to authentication.

189. Furthermore, Chivallier explicitly discloses that “data concerning the user health parameters” are first encrypted using the public and private encryption keys exchanged in an authentication step prior to transmission of analyte data:

The authentication process uses a dual key handling secure process with a private and public key encryption through the well-known RSA

encryption algorithm with digital signatures and certificates. The authentication process can occur between the sensor module 202 and the mobile device 300. The process may use the sensor private key stored in the SE 209 of the sensor module 202 and the public key stored in the SE 309 of the NFC tag reader 308 to enable authentication. The public key in the SE 309 is used to recognize and authenticate the private key of sensor 202 by means of the certificates. At the end of the mutual authentication process, if there is a matching between the private stored key in the NEC tag 209 of the sensor module 202 and the public stored key in the NFC tag reader 308, the sensor module 202 is fully authenticated as being the sensor module 202 compatible with the mobile device 300. ***Thereafter any communication between the sensor 202 and mobile device 300, in accordance with the private and public keys, will be encrypted so all data will only be readable by the sensor 202 and device 300.***

Ex. 1008 at [0029].

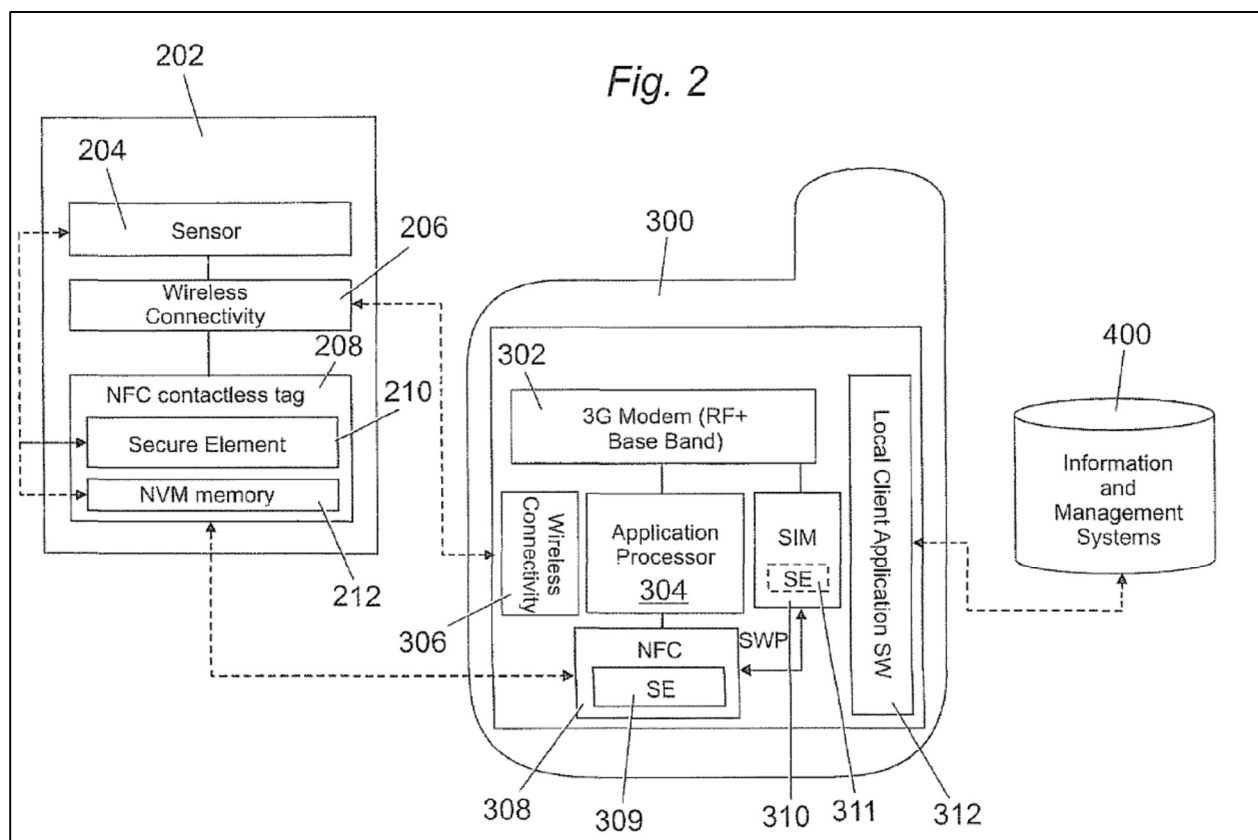
190. In the Hernandez-Rosas-Chivallier combination, the CGM sensor and display device use a first wireless protocol to exchange the information related to authentication, where the information related to authentication is subsequently used to encrypt the analyte data for secure communication to the sensor device over a second wireless protocol.

h) 14[g] “wherein the first wireless protocol is different than the second wireless protocol, and”

191. Hernandez-Rosas in view of Chivallier suggests this limitation.

192. As noted in claims 14[b] and 14[e], Hernandez-Rosas discloses that the wireless data communication may utilize any number of protocols, including Wi-Fi, Bluetooth, and Bluetooth Low Energy protocols. Ex. 1007 at [0160]. However, Hernandez-Rosas does not explicitly recite that the wireless protocol used during the first interval and second interval are different protocols.

193. Chivallier explicitly teaches a CGM system where an exchange of information related to authentication occurs via NFC, while the wireless communication of health information occurs via a separate wireless module that can be Bluetooth, ZigBee, ultra-wide band, or “any other appropriate means”:



The sensor 204 connects to a wireless connectivity module 206. The connection between the sensor 204 and the module 206 can be *a Bluetooth™ connection, a ZigBee™ connection, an ultra-wide band connection or any other appropriate means. ...*

The wireless connectivity module 206 also connects to a tag 208. The tag 208 is a Near Field Communication (NFC) contactless tag. The tag 208 is a passive label, which comprises specific data. In the present invention, data relates to the sensor device 102 and also to the health parameters measured on the user 100 with the sensor 204. *The data stored in the tag 208 can be read using a NFC module through Radio Frequency Identification (RFID) in combination with a corresponding NFC contactless tag reader.* The tag reader belongs to another device such as the mobile device 300. The tag 208 includes a secure element (SE) 210 and a non-volatile memory (NVM) 212.

Ex. 1008 at Fig. 2, [0016]-[0017].

194. In the Hernandez-Rosas-Chivallier combination, the CGM sensor and display device use a first wireless protocol to exchange the information related to authentication and subsequently use a different, second wireless protocol to transmit encrypted analyte data to the display device (*e.g.*, the first wireless protocol is NFC, while the second wireless protocol is Bluetooth).

- i) 14[h] “neither initiating transmission of analyte values to the display device nor providing a notification on the display device when the information related to authentication was not exchanged during the first interval.”

195. Hernandez-Rosas discloses this limitation.

196. Hernandez-Rosas discloses that authentication is “required” prior to communicating data between the sensor and the display device:

In certain embodiments, one or more display devices comprise built-in authentication mechanisms, wherein *authentication is required for communication between the sensor electronics module and the display device.*

Ex. 1007 at [0119]; *see also id.* at [0149] (“an authentication procedure needs to be performed as part of a data connection process 414.”), [0150] (“Once authenticated, the analyte sensor system 8 and display device 110, 120, 130, 140 may exchange information.”).

197. A POSITA would have understood that Hernandez-Rosas’s disclosure describing how the analyte data is not sent over the wireless connection unless the sensor and display device have been authenticated discloses that the display device would not display any notifications or alerts because the display device must first receive analyte data before making any determinations to display alerts or notifications based on analyte data.

198. Similarly, Chivallier also discloses that data is “only transmitted after authentication” in order to provide a high-level of security for the user data:

One of the particular advantages of the present invention is the fact that the sensor has stored thereon a private encryption key which is used to authenticate the sensor with a receiver (i.e., mobile device). Also the private encryption key ensures that all data that “leaves” the patient or

user is encrypted. *Before authentication all data is stored on the sensor and is only transmitted after authentication.* This provides a very high level of security for the user data. This is essential for patient confidentiality [sic] and medical/patient acceptance of wireless communication as a means for transmitting medical and other private data.

Ex. 1008 at [0034]. Chivallier further discloses that the system can “provide an alert if the analysis [of the transmitted data] provides a critical result for the health of the patient.” *Id.* at [0002]. Because Chivallier discloses that the alerts shown to the user are based on an analysis of the data transmitted by the sensor (*id.*), and because Chivallier teaches that the sensor data is not transmitted to the mobile device without authentication, Chivallier discloses neither initiating transmission of analyte values to the display device nor providing a notification on the display device when the information related to authentication was not exchanged during the first interval.

3. Claim 15

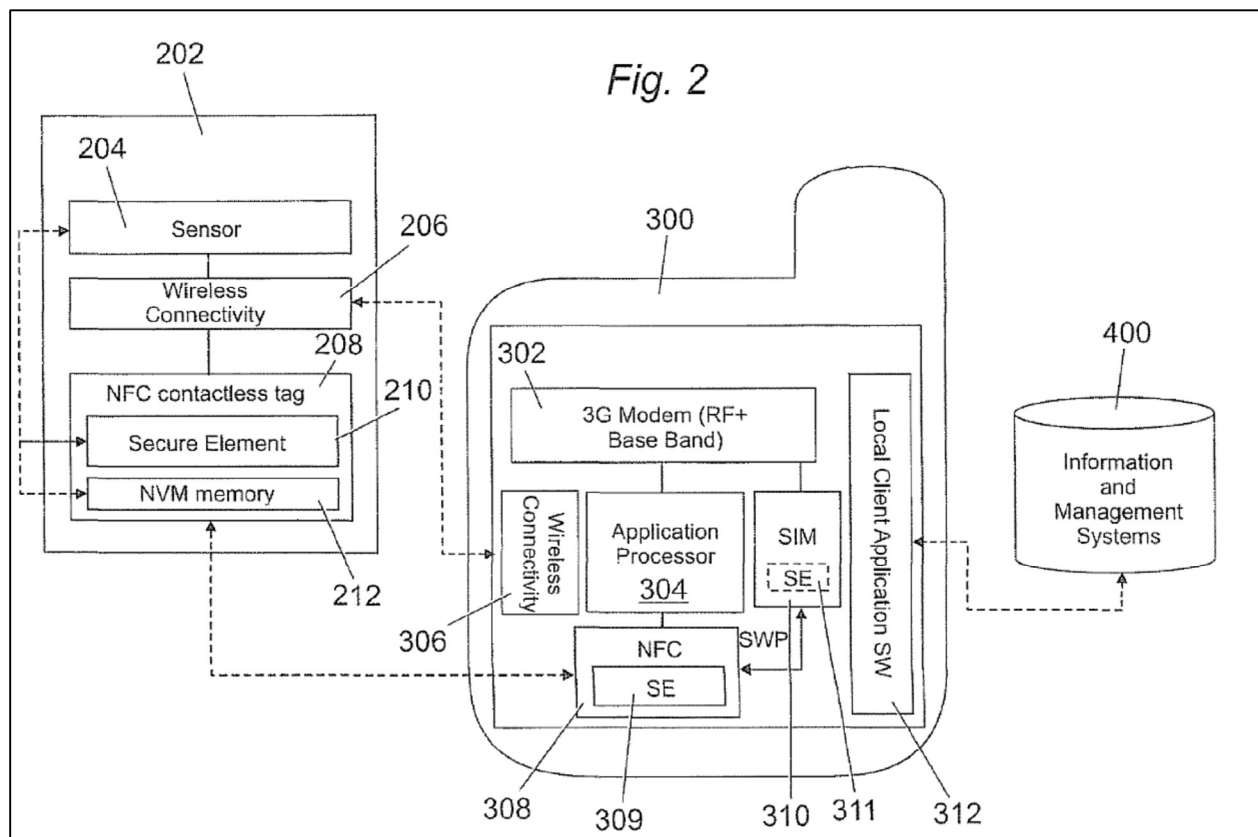
199. Claim 15 depends from claim 14. As explained above the combination of Hernandez-Rosas and Chivallier renders obvious claim 14 as a whole. *See, supra*, claim 14.

a) 15[a] “wherein the first wireless protocol is selected from the group consisting of: WiFi communication, Near Field Communication (NFC) and Bluetooth Low Energy (BLE) communication; and”

200. Hernandez-Rosas in view of Chivallier suggests this limitation.

201. As noted in claim 14[g], Hernandez-Rosas discloses that the wireless data communication may utilize any number of protocols, including Wi-Fi, Bluetooth, and Bluetooth Low Energy protocols.

202. Chivallier explicitly teaches a CGM system where the “first wireless protocol” used for the exchange of information related to authentication is NFC:



The wireless connectivity module 206 also connects to a tag 208. The tag 208 is a Near Field Communication (NFC) contactless tag. The tag 208 is a passive label, which comprises specific data. In the present invention, data relates to the sensor device 102 and also to the health parameters measured on the user 100 with the sensor 204. ***The data stored in the tag 208 can be read using a NFC module through Radio***

Frequency Identification (RFID) in combination with a corresponding NFC contactless tag reader. The tag reader belongs to another device such as the mobile device 300. The tag 208 includes a secure element (SE) 210 and a non-volatile memory (NVM) 212.

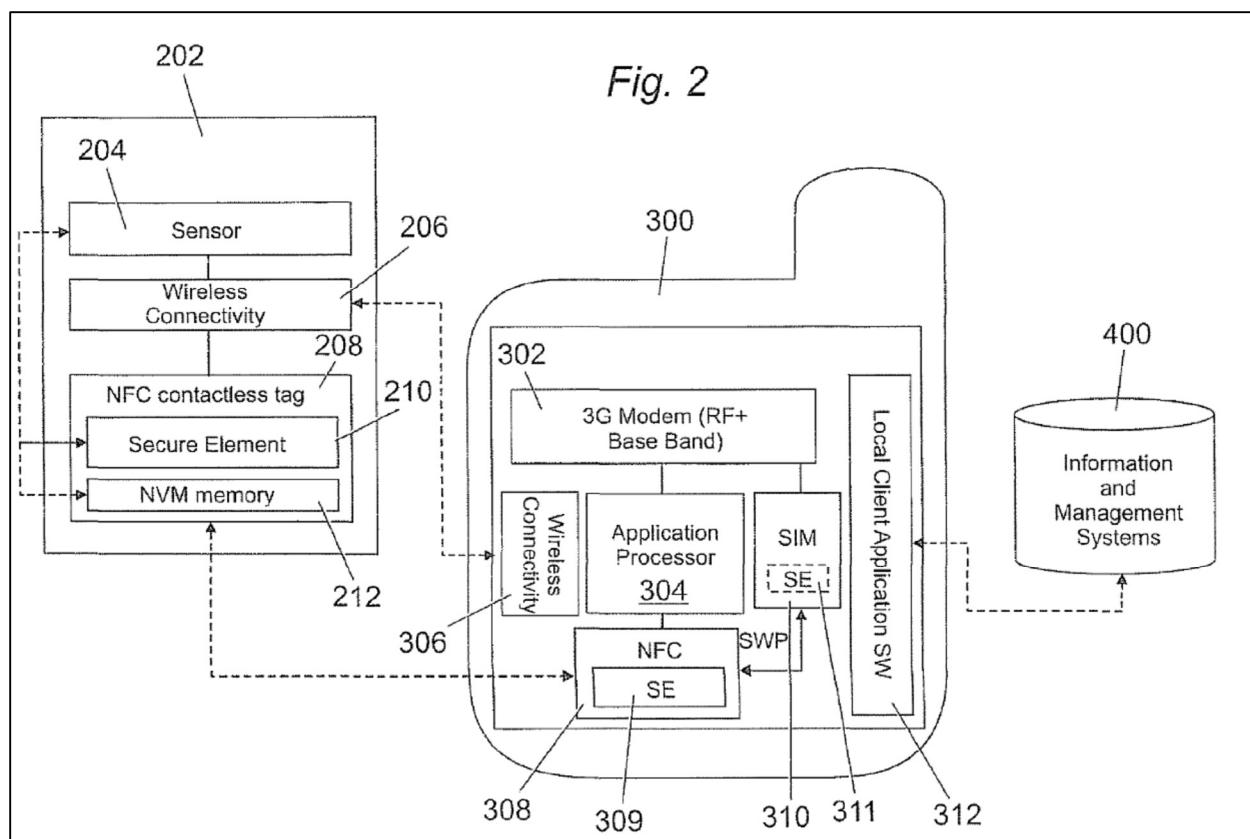
Ex. 1008 at Fig. 2, [0017].

b) 15[b] “wherein the second wireless protocol is selected from a group consisting of: WiFi communication, NFC and BLE communication.”

203. Hernandez-Rosas in view of Chivallier suggests this limitation.

204. As noted in claim 14[g], Hernandez-Rosas discloses that the wireless data communication may utilize any number of protocols, including Wi-Fi, Bluetooth, and Bluetooth Low Energy .

205. Chivallier explicitly teaches a CGM system where the wireless communication of health information occurs using Bluetooth, ZigBee, ultra-wide band, or “any other appropriate means”:



The sensor 204 connects to a wireless connectivity module 206. The connection between the sensor 204 and the module 206 can be *a Bluetooth™ connection, a ZigBee™ connection, an ultra-wide band connection or any other appropriate means*. The module 206 is a communication module typically having an ultra-low power requirement. The module 206 may connect to another wireless connectivity module located in another device such as the mobile device 300. Thus, the module 206 allows wireless connection of the sensor 204 with another device.

Ex. 1008 at Fig. 2, [0016].

4. Claim 16

206. Claim 16 depends from claim 14. As explained above the combination of Hernandez-Rosas and Chivallier renders obvious claim 14 as a whole. *See, supra*, claim 14.

a) 16[a] “wherein the analyte sensor system is a continuous glucose sensor system and”

207. Hernandez-Rosas discloses this limitation.

208. Hernandez-Rosas discloses a CGM system.

In some embodiments, *a system is provided for continuous measurement of an analyte in a host* that includes: a continuous analyte sensor configured to continuously measure a concentration of the analyte in the host and a sensor electronics module physically connected to the continuous analyte sensor during sensor use.

Ex. 1007 at [0104].

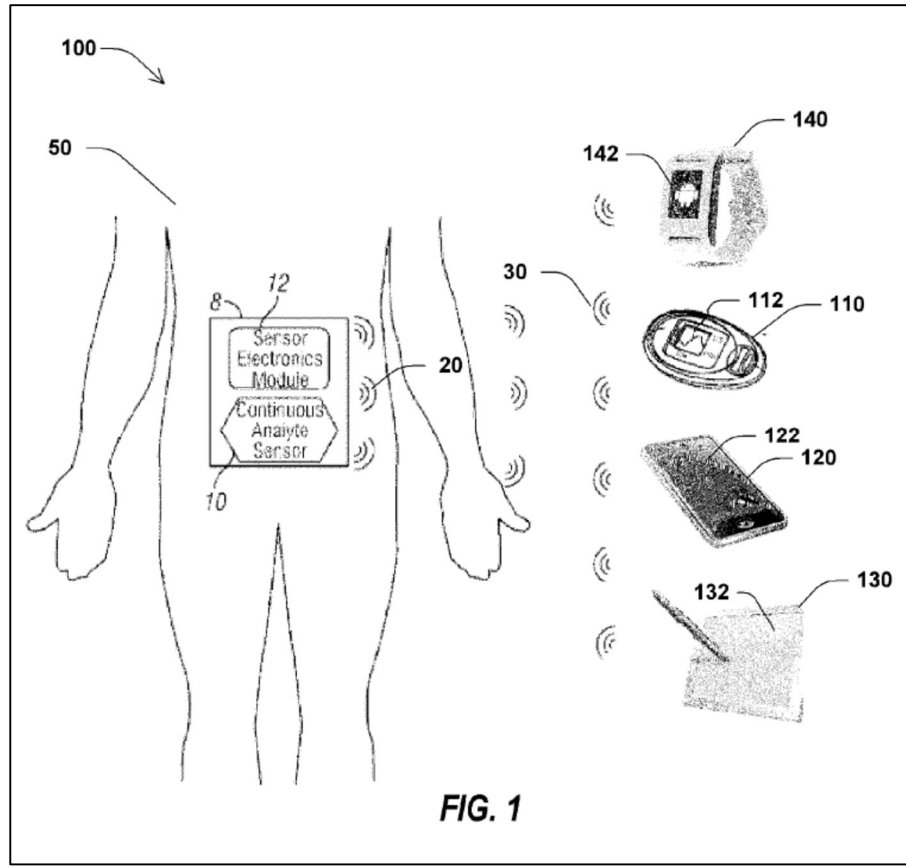


FIG. 1 is a diagram depicting an *exemplary continuous analyte monitoring system 100* including an analyte sensor system 8 and a plurality of display devices 110, 120, 130, 140 according to certain aspects of the present disclosure. The analyte sensor system 8 includes a sensor electronics module 12 and *a continuous analyte sensor 10* associated with the sensor electronics module 12.

Id. at [0124], Fig. 1; *see also id.* at [0125].

b) 16[b] “the information related to authentication comprises an application key.”

209. Hernandez-Rosas discloses this limitation.

210. As explained above in claim 14[b], Hernandez-Rosas discloses that during the authentication process the sensor and control device exchange a “challenge value” and a “hash value based on the challenge value and the identification information associated with the analyte sensor.” *See, supra*, claim 14[b]. As explained in the '222 patent, the claimed “application key” can be derived by an exchange of challenge and hash values. Ex. 1001 at 61:67-62:4. Accordingly, Hernandez-Rosas discloses the information related to authentication comprises an application key.

5. Independent Claim 18

211. The combination of Hernandez-Rosas and Chivallier renders obvious claim 18 obvious as a whole.

a) 18[Pre] “An analyte sensor system configured for wireless communication of analyte data, the analyte sensor system comprising:”

212. Hernandez-Rosas discloses the preamble, to the extent it is limiting.

213. To the extent the preamble is limiting, Hernandez-Rosas discloses a CGM system for wireless communication of analyte data. *See, supra*, claim 14[Pre].

b) 18[a] “a continuous analyte sensor configured to measure analyte values in a host;”

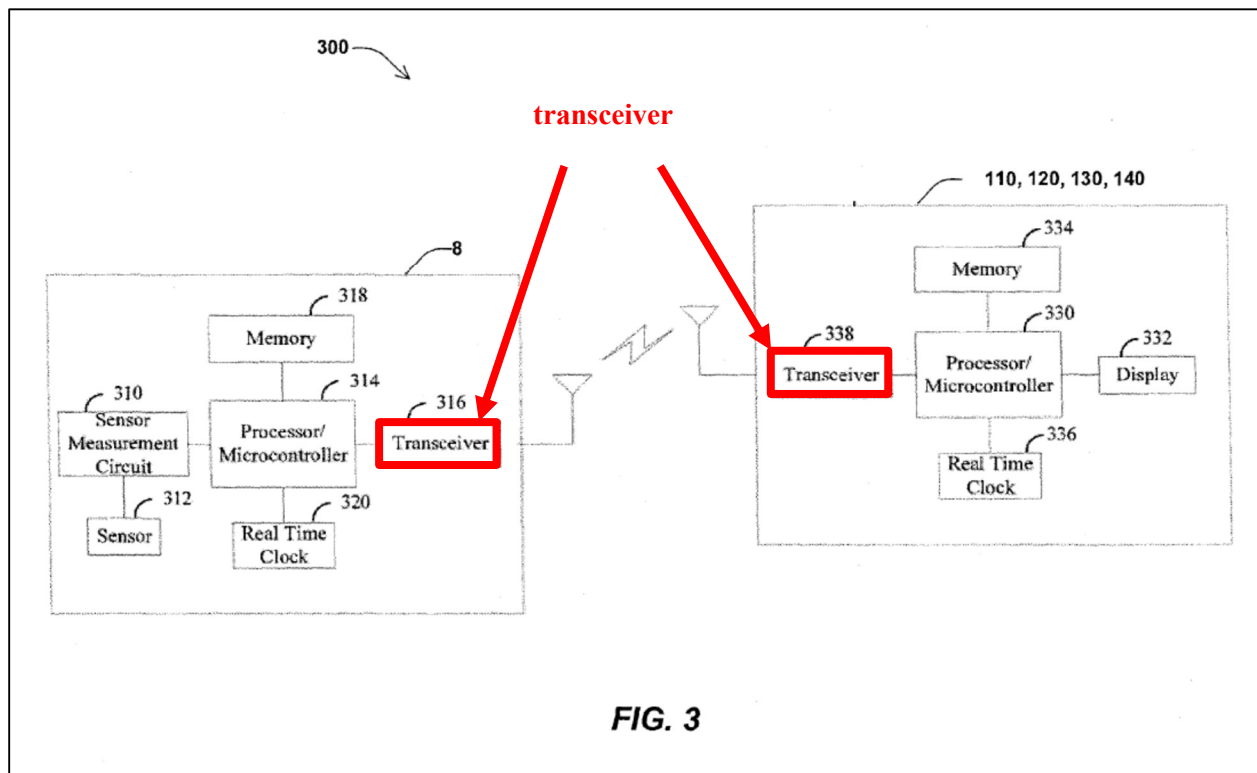
214. Hernandez-Rosas discloses this limitation.

215. *See, supra*, claim 14[a].

c) 18[b] “a transceiver configured to transmit and receive wireless signals; and”

216. Hernandez-Rosas discloses this limitation.

217. Hernandez-Rosas discloses a CGM with the sensor 8 and display devices 110, 120, etc. each having a transceiver configured to transmit and receive wireless signals.

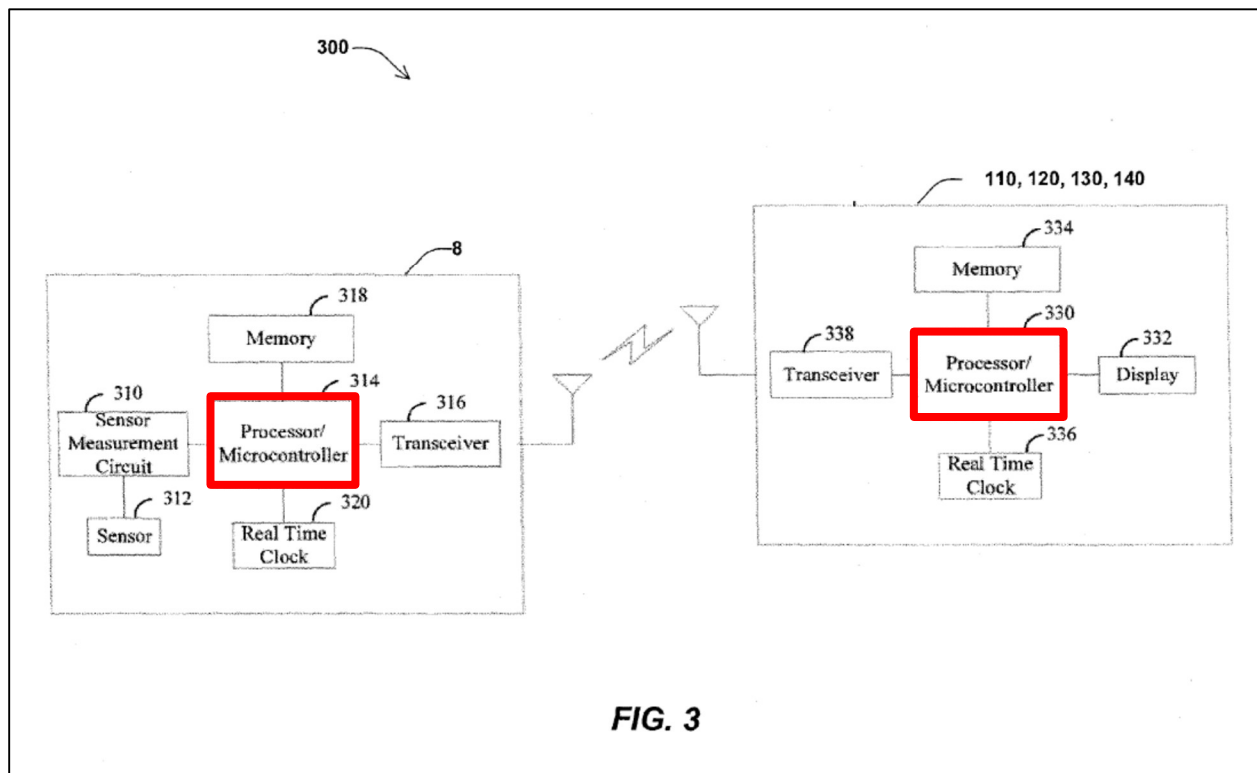


Ex. 1007 at Fig. 3 (annotated); *see also id.* at [0139] (“The processor may be further coupled to *a radio unit or transceiver 316*”), [0142] (“The display device 110, 120, 130, 140 may further include a *radio unit or transceiver 338* for receiving sensor data and for sending requests, instructions, and data to the analyte sensor system 8.”).

d) 18[c] “a processor operatively coupled to the analyte sensor and the transceiver and configured to cause the analyte sensor system to:”

218. Hernandez-Rosas discloses this limitation.

219. Hernandez-Rosas discloses that both the sensor and the display device contain processors (annotated below in red) operably coupled to the analyte sensor and transceivers.



Ex. 1007 at Fig 3 (annotated).

The analyte sensor system 8 may include an analyte sensor 312 (also designated 10 in FIG. 1) coupled to a sensor measurement circuit 310 for processing and managing sensor data. The sensor measurement circuit 310 may be coupled to a processor 314 (part of item 12 in FIG. 1). In some embodiments, the processor 314 may perform part or all of the functions of the sensor measurement circuit 310 for obtaining and

processing sensor measurement values from the sensor 312. The processor may be further coupled to a radio unit or transceiver 316 (part of item 12 in FIG. 1) for sending sensor data and receiving requests and commands from an external device, such as the display device 110, 120, 130, 140, which is used to display or otherwise provide the sensor data to a user.

Id. at [0139]; *see also id.* at [0142] (“The display device 110, 120, 130, 140 may be used for alerting and providing sensor information to a user, and may include a processor 330 for processing and managing sensor data. ... The instructions may be executed by the processor 330 to control and manage the transceiver 338.”).

220. The processor 330 in the display device(s) controls the operation of the display device and is configured to cause the display device to exchange the information related to authentication with the sensor device, authenticate the sensor device, receive encrypted analyte data from the sensor, and to control the display. Ex. 1007 at [0142]. Similarly, the controller 314 in the CGM sensor 8 controls the operation of the sensor and is configured to cause the sensor to exchange the authentication information with the display device, receive measurements from the glucose sensor, and transmit encrypted analyte data to the display device. *Id.* at [0139]. A POSITA would thus understand that the processors 330, 314 in Hernandez-Rosas are configured to cause the CGM system to perform the functions discussed below in claim elements 18[d]-18[j].

e) 18[d] “during a first interval, establish a first connection between the analyte sensor system and a display device;”

221. Hernandez-Rosas discloses this limitation.

222. As explained above in claim 14[b], Hernandez-Rosas discloses establishing a first connection during a first interval for exchanging information related to authentication between a sensor and a display device. *See, supra*, claim 14[b].

f) 18[e] “during the first connection, exchange information related to authentication between the analyte sensor system and the display device;”

223. Hernandez-Rosas discloses this limitation.

224. As explained above in claim 14[b], Hernandez-Rosas discloses exchanging information related to authentication with a display device during a first interval. *See, supra*, claim 14[b].

g) 18[f] “perform a first determination whether authentication was performed during the first interval;”

225. Both Hernandez-Rosas and Chivallier disclose this limitation.

226. As explained above in claim 14[h], Hernandez-Rosas discloses that authentication is “required” prior to communicating data between the sensor and the display device. *See, supra*, claim 14[h]. Hernandez-Rosas further discloses that the sensor “verifies” the received identification from the display device and, if successfully verified, sends a signal confirming the authentication to the display device.

The transceiver 316 receives the hash value from the display device 110, 120, 130, 140, decodes the identification information from the hash value, and *verifies that the received identification information matches identification information associated with the sensor system 8* and/or transceiver 316 previously stored in the memory 318 of the analyte sensor system 8, such as during manufacturing of the sensor system 8. *Upon verification, the transceiver 316 sends a signal confirming a successful authentication to the display device 110, 120, 130, 140.*

Ex. 1007 at [0150], Fig. 4. The verification of the authentication information corresponds to the claimed “first determination whether authentication was performed during the first interval.”

227. Similarly, as explained above in claim 14[h], Chivallier also discloses that data is “only transmitted *after* authentication” in order to provide a high-level of security for the user data. *See, supra*, claim 14[h]. The determination of whether the sensor and mobile device have successfully performed authentication prior to transmitting user data also corresponds to the claimed “first determination whether authentication was performed during the first interval.”

h) 18[g] “perform a second determination whether one or more alerts indicative of a medical condition of the host is to be triggered based on the measured analyte data;”

228. Hernandez-Rosas discloses this limitation.

229. *See, supra*, claim 14[c].

- i) 18[h] “trigger at least one alert and provide a notification on the display device when the second determination indicates that the at least one alert is to triggered indicative of the medical condition of the host; and”
230. Hernandez-Rosas discloses this limitation.
231. *See, supra*, claim 14[d].
- j) 18[i] “during a second interval, transmit an encrypted analyte value to the display device, when the first determination indicates that the authentication was performed during the first interval, and”
232. Hernandez-Rosas discloses this limitation.
233. *See, supra*, claim 14[e].
- k) 18[j] “neither initiate transmission of analyte values to the display device if nor provide a notification on the display device when the first determination indicates that the authentication was not performed during the first interval.”
234. Hernandez-Rosas discloses this limitation.
235. *See, supra*, claim 14[h].

6. Claim 19

236. Claim 19 depends from claim 18. As explained above, the combination of Hernandez-Rosas and Chivallier renders obvious claim 18 as a whole. *See, supra*, claim 18.

- a) 19[a] “wherein the processor is further configured to cause the analyte sensor system to: during the second interval, establish a second connection between the analyte sensor system and the display device; and”
237. Hernandez-Rosas discloses this limitation.

238. As explained above in claim 14[e], Hernandez-Rosas discloses establishing a second connection between the sensor and display device during a second interval. *See, supra*, claim 14[e].

b) 19[b] “during the second connection, bypass the exchange of the information related to authentication.”

239. Hernandez-Rosas discloses this limitation.

240. *See, supra*, claim 14[e].

7. Claim 20

241. Claim 20 depends from claim 19. As explained above, the combination of Hernandez-Rosas and Chivallier renders obvious claim 19 as a whole. *See, supra*, claim 19.

a) 20[a] “wherein the analyte sensor system is a continuous glucose sensor system, and”

242. Hernandez-Rosas discloses this limitation.

243. *See, supra*, claim 16[a].

b) 20[b] “the information related to authentication comprises an application key”

244. Hernandez-Rosas discloses this limitation.

245. *See, supra*, claim 16[b].

c) 20[c] “wherein the processor is further configured to cause the analyte sensor system to use the application key to encrypt an analyte value including a glucose value measured by the continuous analyte

sensor to generate the encrypted analyte value including an encrypted glucose value, and”

246. Hernandez-Rosas discloses this limitation.

247. As explained in claim 14[b], Hernandez-Rosas discloses that the “hash” value exchanged during the first interval is “based on the challenge value and the identification information associated with the analyte sensor system 8,” and as explained in claim 16[b] this hash value of the challenge value and identification information corresponds to the “application key.” *See, supra*, claims 14[b], 16[b]. Hernandez-Rosas discloses that this information relating to identification can be used to encrypt the analyte data in a CGM system. *See, supra*, claim 14[f]. Accordingly, Hernandez-Rosas discloses or suggests the processor is configured to encrypt analyte values using the application key including a glucose value measured by the continuous analyte sensor to generate the encrypted analyte value including an encrypted glucose value.

d) 20[d] “wherein the use of the application key allows the analyte sensor system to bypass the exchange.”

248. *See, supra*, claim 14[e].

IX. AVAILABILITY FOR CROSS-EXAMINATION

249. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross examination in the case and that cross examination will take place within the

United States. If cross examination is required of me, I will appear for cross examination within the United States during a time as mutually agreed between the parties.

X. RIGHT TO SUPPLEMENT

250. I reserve the right to supplement my opinions in the future to respond to any arguments that the Patent Owner raises. This declaration represents only those opinions that I have formed to date. I reserve the right to revise, supplement, and/or amend my opinions stated herein based on new information that becomes available to me and on my continuing analysis of the materials already provided.

XI. CONCLUSION

251. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

April 9, 2024
Date



Sayfe Kiaei, Ph.D.