

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ABBOTT DIABETES CARE INC.,
Petitioner,

v.

DEXCOM, INC.,
Patent Owner.

IPR2024-00797
Patent 10,375,222 B2

Before MITCHELL G. WEATHERLY, JON M. JURGOVAN, and
FREDERICK C. LANEY, *Administrative Patent Judges*.

JURGOVAN, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Petitioner Abbott Diabetes Care Inc. filed a Petition (Paper 1, “Pet.”) pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 14–16 and 18–20 (“the challenged claims”) of U.S. Patent No. 10,375,222 B2 (Ex. 1001, “the ’222 patent”).

Patent Owner DexCom, Inc. filed a Preliminary Response (Paper 6, “Prelim. Resp.”). Patent Owner argues that the Petition fails to satisfy the requisite threshold for instituting review on the merits.

For reasons provided below, we determine on behalf of the Director (*see* 37 C.F.R. § 42.4(a)) that the record demonstrates a reasonable likelihood that Petitioner would prevail with respect to at least one of the challenged claims on the merits, so we grant institution of the petitioned *inter partes* review. *See* 35 U.S.C. § 314(a).

II. BACKGROUND

A. *Real Parties-in-Interest and Related Proceedings*

Petitioner identifies itself (i.e., Abbott Diabetes Care Inc.) and Abbott Diabetes Care Sales Corp. and Abbott Laboratories. Petitioner is directly owned by Abbott Laboratories, and Petitioner directly owns Abbott Diabetes Care Sales Corp. Pet. 2. Patent Owner identifies itself (i.e., DexCom, Inc.) as the real party-in-interest. Paper 3, 1.

Petitioner identifies the following district court litigation as related to this proceeding: *Abbott Diabetes Care Inc. et al. v. DexCom, Inc.*, Case No. 1:23-cv-00239 (D. Del.). Pet. 2–3. Patent Owner identifies the following *inter partes* review proceedings concerning patents asserted by Patent Owner in the district court litigation as related to this proceeding: IPR2024-00840 (U.S. Patent No. 9,119,528 B2); IPR2024-00841 (U.S.

Patent No. 10,709,364 B2); IPR2024-00853 (U.S. Patent No. 11,213,204 B2); IPR2024-00859 (U.S. Patent No. 11,510,625 B2); IPR2024-00860 (U.S. Patent No. 11,510,625 B2); IPR2024-00861 (U.S. Patent No. 9,801,541 B2); IPR2024-00890 (U.S. Patent No. 11,020,031 B1); and IPR2024-00891 (U.S. Patent No. 11,020,031 B1). Paper 3, 2.

B. The '222 Patent

The '222 patent is titled “System and Method for Wireless Communication of Glucose Data.” Ex. 1001, code (54). The '222 patent relates to authentication and encryption of communications between a sensor for continuous measurement of an analyte, such as glucose, in a host, and a display device for displaying related information. *Id.*, code (57), 33:24–41.

Figure 1A of the '222 patent is shown below.

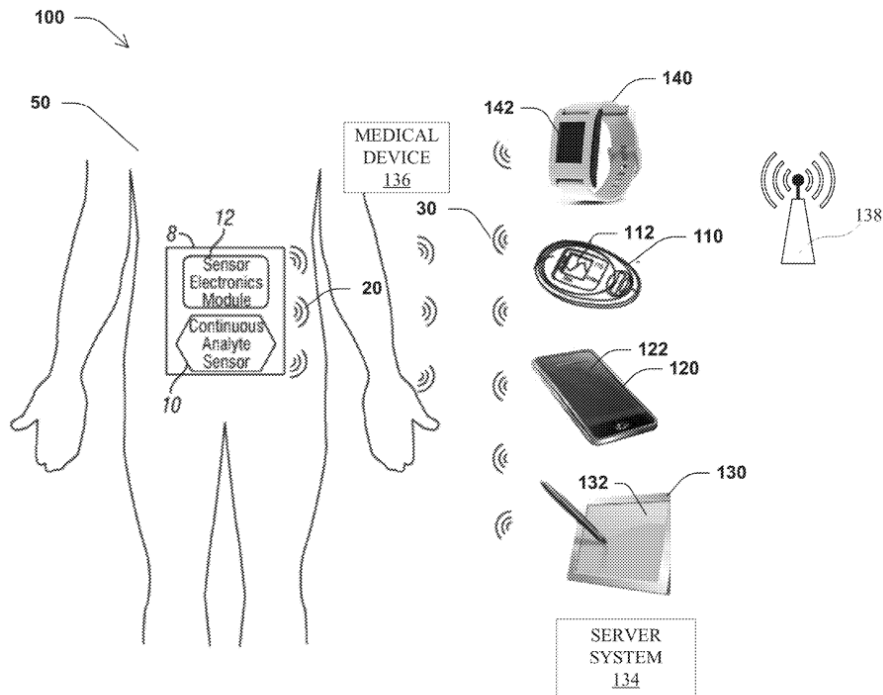


FIG. 1A

Figure 1A above shows a system 100 with an analyte sensor system 8 wirelessly communicating with display devices 110, 120, 130, 140. *Id.* at 41:56–42:11.

Analyte sensor system 8 includes continuous analyte sensor 10 and sensor electronics module 12. *Id.* at 41:64–67. Analyte sensor 10 may be an implantable continuous glucose sensor. *Id.* at 40:17–45. Sensor electronics module 12 includes hardware, firmware and/or software that enables measurement of levels of the analyte via a glucose sensor. *Id.* at 42:20–22. Sensor electronics module 12 provides analyte data to the display devices 110, 120, 130, 140. *Id.* at 41:67–42:3, 42:46–55.

Display devices 110, 120, 130, 140 are configured for displaying sensor information and analyte data to a user, and receiving inputs from the user. *Id.* at 42:46–55. Display devices 110, 120, 130, and 140 may be a custom device, mobile phone, tablet, and smart watch, respectively, as shown in Figure 1A. *Id.* at 43:29–43.

Figure 7A of the '222 patent is shown below.

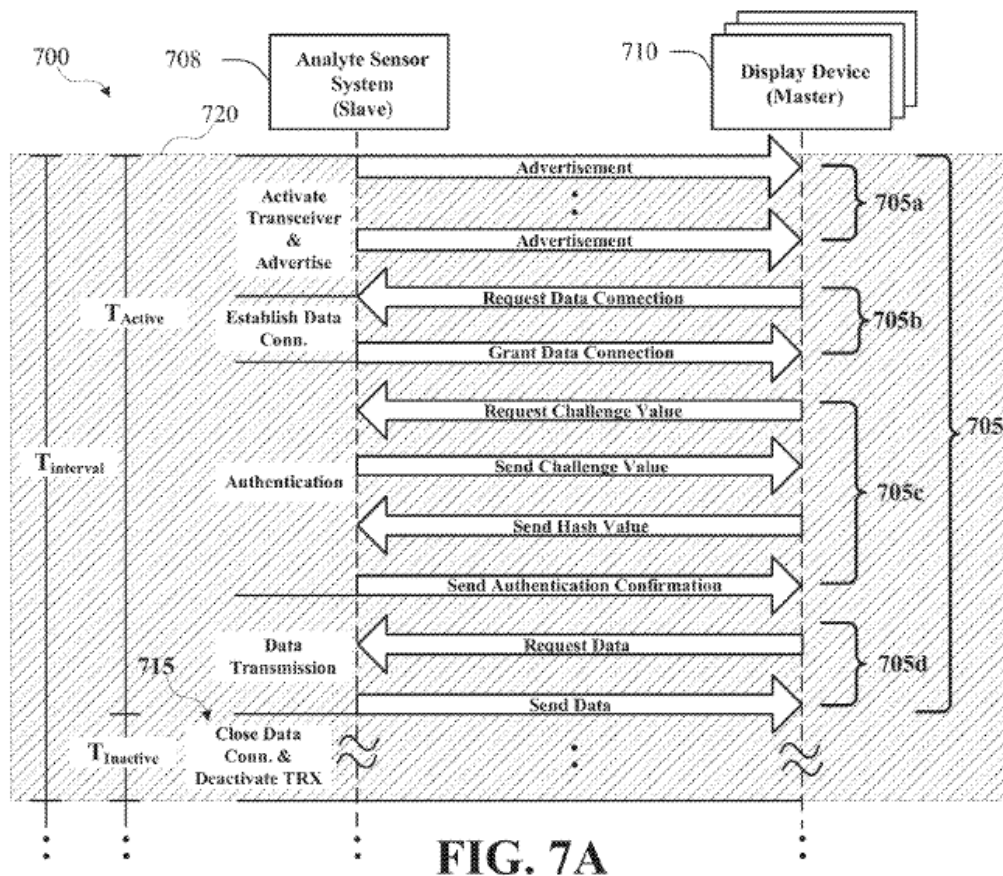


FIG. 7A

Figure 7A is a flow diagram showing method 700 for wireless communication of analyte data between analyte sensor system 708 and display device 710 during communication session 720. *Id.* at 58:51–55.

In operation 705a, analyte sensor system 708 transmits advertisement messages, which display device 710 receives. *Id.* at 60:18–21. Display device 710 may listen or scan continuously for advertisement messages transmitted by analyte sensor system 708. *Id.* at 60:18–21.

In operation 705b, in response to an advertisement message, display device 710 requests a data connection with analyte sensor system 708. *Id.* at 60:37–42.

In operation 705c, an authentication procedure involves the exchange of various messages between analyte sensor system 708 and display device

710. *Id.* at 60:44–51. As shown in Figure 7A, the messages exchanged may include “request challenge value,” “send challenge value,” “send hash value,” and “send authentication confirmation.” *Id.* at 60:52–61:12.

In operation 705d, connected display device 710 may request and receive desired information (e.g., analyte data, control information, identification information, and/or instruction) from analyte sensor system 708. *Id.* at 63:40–47.

C. Overview of Challenged Claims

Claims 14–16 and 18–20 are challenged in this proceeding. Pet. 4. Claim 14 is a method, and claim 18 is a system that is functionally similar to claim 14. Claims 15 and 16 depend from claim 14, and claims 19 and 20 depend from claim 18.

Claim 14, which is representative, is shown below with limitation identifiers indicated in brackets and disputed claim language emphasized in italics.

14. [Pre] A method for wireless communication of analyte data, the method comprising:
 - [a] measuring analyte values in a host using a continuous analyte sensor of an analyte sensor system;
 - [b] during a first interval, using a first wireless protocol to perform an exchange of *information related to authentication* with a display device;
 - [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;
 - [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 triggered indicative of the medical condition of the host; and

[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, 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 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.

Ex. 1001, 116:58–117:15 (emphases added).

D. Asserted Prior Art

Petitioner relies on the following four references as prior art against claims 14–16 and 18–20 of the '222 patent. Pet. 4.

Name	Reference	Exhibit No.
Yarger	US 2014/0313052 A1	1005
Love	US 2015/0207796 A1	1006
Hernandez-Rosas	US2015/0123810 A1	1007
Chivallier	US2010/0045425 A1	1008

Patent Owner does not dispute that these references are prior art against claims 14–16 and 18–20 of the '222 patent. *See generally* Prelim. Resp.

E. Asserted Grounds

Petitioner asserts the following grounds of unpatentability. Pet. 4.

Ground	Reference(s)/Basis	35 U.S.C. § ¹	Claim(s) Challenged
1	Yarger, Love	103	14–16, 18–20
2	Hernandez-Rosas, Chivallier	103	14–16, 18–20

F. Testimonial Evidence

Petitioner relies on the proffered expert witness testimony of Dr. Sayfe Kiaei (Exhibit 1003). Patent Owner does not rely on opposing expert witness testimony. *See generally* Prelim. Resp.

III. PETITIONER’S GROUNDS OF UNPATENTABILITY

A. Legal Standards

Before considering Petitioner’s and Patent Owner’s contentions, we address in this section legal standards relevant to this proceeding.

1. Petitioner’s Burden

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review

¹ Amendments to 35 U.S.C. § 103 enacted by the Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”) took effect on March 16, 2013. The ’222 patent claims priority to U.S. Provisional Application 62/364,771 filed July 20, 2016. Ex. 1001, code (60). Therefore, we apply the AIA version of § 103.

petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”). This burden of persuasion never shifts to the patent owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

2. *Obviousness*

A patent claim is unpatentable under 35 U.S.C. § 103 if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art (“POSITA”) to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness.² *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. *Level of Ordinary Skill in the Art*

In determining the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (internal quotation marks and citation omitted). The applied prior art may

² Neither Petitioner nor Patent Owner have submitted any such objective evidence in the record at this time.

reflect an appropriate level of skill. *Okajima v. Bourdeau*, 261 F.3d 1350, 1354–55 (Fed. Cir. 2001).

Petitioner asserts that

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.

Pet. 10–11.

Patent Owner does not address Petitioner’s proposed level of ordinary skill in the art. *See generally* Prelim. Resp.

Petitioner’s proposed level of skill in the art is consistent with the ’222 patent and the asserted prior art except that we set the level to “two . . . years of experience” because the qualifier “or more” would render the level ambiguous. Otherwise, we agree with and will use Petitioner’s proposed level for this Decision.

C. Claim Construction

We interpret the ’222 patent claims “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b). This “includ[es] construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.*

“Petitioner does not believe that any specialized constructions are necessary” for this proceeding. Pet. 11. However, Petitioner asserts that “[t]he ’222 patent claims make clear that the ‘information related to authentication’ can comprise an ‘application key’” which “can comprise a random number” or “can include a challenge and hash value.” *Id.* at 11–12 (citing Ex. 1001, 61:62–63, 61:67–62:4, 62:15–16). Thus, Petitioner asserts that “the claim terms ‘information related to authentication’ and ‘application key’ both at least encompass (i) a random number and (ii) exchange of challenge and hash values, related to identification of the sensor device or the display device.” *Id.* at 12. Although the file history of the ’222 patent indicates that the examiner and applicant discussed the claimed “information related to authentication” during an interview (Ex. 1002, 380), there is no indication in the file history that any particular meaning or definition was given to the phrase.

Patent Owner asserts that, in accordance with its ordinary meaning, “authentication involves validating authorization.” Prelim. Resp. 1, 20–21. Patent Owner argues that Petitioner improperly equates “authentication” with “identification” with no evidence to support its assertion. *Id.* at 31–32. Specifically, Patent Owner contends that

It is well understood that identification and authentication are different things. Identification information for a device (or user) is information that uniquely identifies the device (or user), whereas authentication information is information used to validate that the device (or user) is an authorized device (or user). [citing *id.* at § III.B; Ex. 1008 ¶¶ 28–29] (“authentication” means validating that a device is authorized as described in the ’222 Patent specification and consistent with the ordinary meaning). For example, in the ubiquitous username and password authentication technique, the username is identification

information that uniquely identifies the user and the password is authentication information that is used to validate that the person seeking to login is an authorized user.

Id. at 32.

We determine that “authentication” and “identification” are well-understood and widely used terms in communications (including wireless), and these terms do not require any specialized constructions for this proceeding.

The ordinary and customary meaning of “authentication” is verifying the identity of communicating devices or users, or, in other words, determining that a device or user is what or who they represent themselves to be. *See, e.g.*, Ex. 1003 ¶¶ 30, 32; Ex. 2002, 175.

“Identification” refers to indicia that uniquely specifies a particular device or user. For example, the ’222 patent discloses that “identification information” can be a serial number of an analyte sensor system. Ex. 1001, 60:6–13; Ex. 2002, 175.

Although “authentication” and “identification” are not synonymous, in the context presented here, they are related concepts and “identification” may be used in the process of “authentication.” For example, the ’222 patent states “[f]or purposes of *authentication*, the analyte sensor system may share an *identification* number with the display device, where the *identification* number is associated with the analyte sensor system.” Ex. 1001, 59:61–67.

On this record, we disagree with Patent Owner’s proposed construction that “authentication involves validating authorization.” As just explained, “authentication” is verifying the identity of communicating devices or users. In contrast, “authorization” relates to rights and privileges

a particular user or device is granted to access a system or resource.

Ex. 2001, 32 (**authentication** A process by which subjects, normally users, establish their identity to a system. This may be effected by the user of a *password or possession of a physical device, e.g., a coded token.”), (“**authorization** A process by which users, having completed an *authentication stage, gain or are denied access to particular resources based on their entitlement”); Ex. 2002, 176. Patent Owner’s proposed construction improperly conflates the concepts of “authentication” and “authorization.

“Authentication” is generally a prerequisite to determining whether a user or device has “authorization” to access a system or device. For example, the ’222 patent states that “*authentication* may be used in attempt to prevent *unauthorized* devices from making a connection.” Ex. 1001, 58:40–45. However, “authentication” of a person or device (i.e., determining that they are who they represent themselves to be) does not necessarily mean that they have “authorization” to access the requested system or device, which requires that they have been granted the necessary access rights and permissions for the requested access.

With these understandings for the claim terms “authentication” and “identification,” consistent with the ordinary and customary meanings of these claim terms, we proceed to consider the grounds asserted by Petitioner against the challenged claims, and Patent Owner’s arguments against Petitioner’s contentions, including Petitioner’s contentions that “information related to authentication” and “application key” are disclosed by the prior art asserted in Petitioner’s challenges.

D. Ground 1: Obviousness over Yarger and Love

Petitioner asserts that claims 14–16 and 18–20 of the '222 patent would have been obvious over the combination of Yarger and Love. Pet. 18–45. Patent Owner disagrees. Prelim. Resp. 16–51.

We conclude that the record demonstrates a reasonable likelihood that Petitioner would prevail with respect to challenged claims 14–16 and 18–20 for the following reasons.

1. Yarger (Ex. 1005)

Yarger is titled “Near Field Telemetry Link for Passing a Shared Secret to Establish a Secure Radio Frequency Communication Link in a Physiological Condition Monitoring System.” Ex. 1005, code (54). Yarger discloses a physiological condition meter and sensor placed in proximity to exchange a secret key using a near field wireless link. *Id.*, code (57). The secret key is used to encrypt data to secure a radio frequency (RF) wireless channel. *Id.*

Yarger’s Figure 1 is shown below.

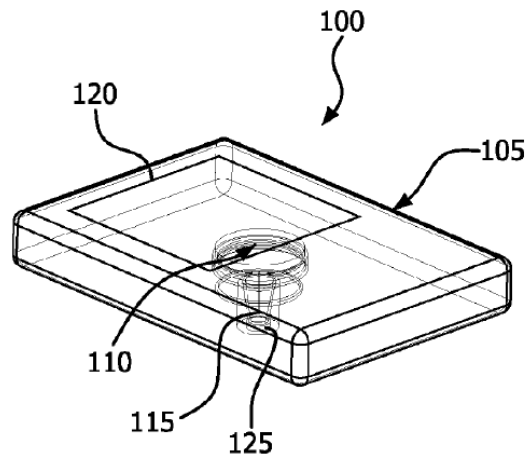


FIG. 1

Yarger's Figure 1 above shows a continuous glucose monitor (CGM) system 100 comprising glucose meter 105 and glucose sensor 110. *Id.* ¶¶ 3, 16. "In operation, the glucose meter 105 and glucose sensor 110 communicate by a radio frequency (RF) wireless link." *Id.* ¶ 16. "To establish the RF wireless link, the glucose meter 105 and the glucose sensor 110 must be linked together (paired) so that the glucose meter 105 only receives information from the paired glucose sensor 110 and not another nearby sensor or other unauthorized device." *Id.* "[T]he glucose sensor 110 and the glucose meter 105 securely exchange a secret key that is used to encrypt information transmitted on a different wireless link." *Id.* "[F]or example, the glucose sensor 110 uses the secret key to encrypt data that is transmitted to the glucose meter 105, which uses an identical secret key to decrypt the encrypted data." *Id.*

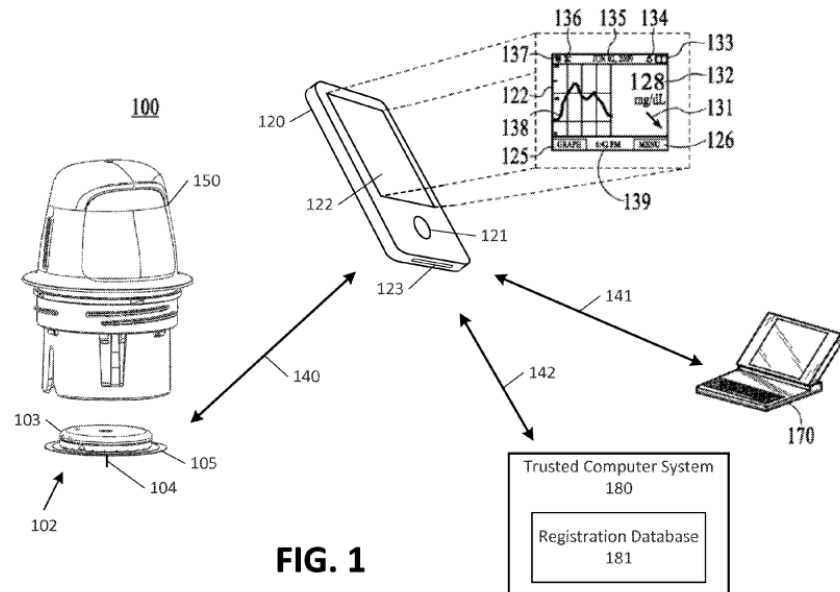
Yarger discloses that "the glucose meter 105 and the glucose sensor 110 preferably include a low power radio link by using inductive coupling of inductors in each device, which is also known as near field communication (NFC)." *Id.* ¶ 18. "[T]he glucose meter 105 and/or glucose sensor 110 exchange a shared key using the NFC wireless link." *Id.* "[T]he shared key is randomly generated data for encrypting communications between the glucose meter 105 and the glucose 110 using a different low power wireless link" which may be "Bluetooth® low power, ZigBee®, a custom wireless link, etc." *Id.* ¶¶ 18, 36.

2. *Love (Ex. 1006)*

Love is titled "Systems, Devices, and Methods for Authentication in an Analyte Monitoring Environment." Ex. 1006, code (54). Love discloses that its systems, devices, and methods allow for authentication of devices

within analyte monitoring systems. *Id.*, code (57). The analyte monitoring systems can be in vivo systems and can include a sensor control device with a sensor and accompanying circuitry, and a reader device for communicating with the sensor control device. *Id.*

Love's Figure 1 is shown below.



Love's Figure 1 above shows an in vivo analyte monitoring system 100 having sensor control device 102 and a reader device 120 that communicate with each other over local communication path (or link) 140, which can be wired or wireless, and uni-directional or bi-directional. *Id.* ¶ 59. Where path 140 is wireless, “a near field communication (NFC) protocol, RFID³ protocol, Bluetooth or Bluetooth Low Energy protocol, Wi-Fi protocol, proprietary protocol, or the like can be used.” *Id.* ¶¶ 18, 59.

“[R]eader device 120 can be configured to output alarms, alert notifications, glucose values, etc., which may be visual, audible, tactile, or any combination thereof.” *Id.* ¶ 70. Reader device 120 may determine the

³ Radio Frequency Identification. Ex. 1006 ¶ 5.

rate of glucose change and output a notification in advance of reaching a clinically significant level (e.g., hyperglycemic or hypoglycemic level). *Id.* ¶¶ 77–78. Reader device 120 may also output a current sensor-derived analyte value, and current rate of analyte change. *Id.* ¶ 98.

3. *Motivation to Combine with Reasonable Expectation of Success*

Petitioner contends that Yarger uses NFC to exchange a secret key between a glucose sensor device and display device, and after validating that exchange, uses a second wireless link to transmit encrypted glucose measurement data from the sensor to the display device. Pet. 19 (citing Ex. 1005, code (57), ¶¶ 6, 32–37, Fig. 4). Petitioner further notes that Yarger discloses that its “CGM system can . . . monitor for ‘physiological conditions,’ such as glycemic conditions, e.g., as part of a ‘diabetes management system.’” *Id.* (citing Ex. 1005, code (57), ¶ 53). Petitioner asserts that “[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 levels.” *Id.* (citing Ex. 1003 ¶¶ 53, 65–67).

Petitioner contends that “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” *Id.* (citing Ex. 1006 ¶ 78) (alteration in original). Petitioner asserts that “Love discloses that its system can be used with a number of different reader devices and wireless protocols.” *Id.* at 19–20 (citing Ex. 1006 ¶¶ 18–19).

Petitioner contends that “[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.’” *Id.* at 20 (citing Ex. 1003 ¶¶ 70–72; Ex. 1005 ¶ 53).

Petitioner further asserts that “[a] POSITA would have had a reasonable expectation of success with adopting the notifications and alarms of Love in the CGM system of Yarger” and that “Yarger’s CGM meter device has a display that already displays glucose levels.” *Id.* (citing Ex. 1005, Fig. 2; Ex. 1003 ¶ 73). Petitioner argues that “[a]dding Love’s notifications and alarms functionality to Yarger’s CGM meter device would simply require adding additional logic to the meter’s programming to compare the current glucose levels against clinically significant thresholds, something a POSITA was well-equipped to do.” *Id.* (citing Ex. 1003 ¶ 73).

Petitioner asserts that “Yarger and Love are analogous art because they are both related to aspects of securely communicating analyte measurements over wireless links in CGM systems.” *Id.* at 20–21 (citing Ex. 1005, code (57); Ex. 1006, code (57); Ex. 1003 ¶ 69; *In re Bigio*, 381 F.3d 1320, 1325–27 (Fed. Cir. 2004)).

Patent Owner does not dispute Petitioner’s contentions that Yarger and Love are analogous, and that a POSITA would have been motivated to combine them with a reasonable expectation of success. *See generally* Prelim. Resp.

We determine that Petitioner shows sufficiently that Yarger and Love are analogous and that a POSITA would have been motivated to combine

them with a reasonable expectation of success. Specifically, Yarger and Love are directed to similar glucose monitoring systems and are thus in the same field of endeavor and address the same problems. *See, e.g.*, Pet. 20–21; Ex. 1005, codes (54, 57), ¶ 1; Ex. 1006, codes (54, 57), ¶ 2. Since Yarger already monitors and displays glucose levels, including clinically significant conditions such as hypoglycemia or hyperglycemia, adding Love’s teaching to generate alarms and notifications for such conditions would improve Yarger’s similar system in the same way as taught by Love. *See, e.g.*, Pet. 19–21; Ex. 1005 ¶¶ 3, 17; Ex. 1006, codes (54, 57), ¶¶ 70, 78. Since this modification merely requires “routine programming” adding logic to compare glucose levels and generate an alarm when a clinically significant threshold is exceeded, a POSITA would have had a reasonable expectation of success in making the modification. *See, e.g.*, Pet. 20; Ex. 1003 ¶ 73. “[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.” *KSR*, 550 U.S. at 417.

Accordingly, on this record, we determine that Petitioner shows sufficiently that a POSITA would have combined the analogous references, Yarger and Love, with a reasonable expectation of success.

4. *Claim 14*

We now consider Petitioner’s and Patent Owner’s contentions with regard to each limitation of claim 14. Pet. 21–36; Prelim. Resp. 16–51. Patent Owner disputes whether “information related to authentication” in limitation 14b is disclosed by the combination of Yarger and Love. Patent Owner does not dispute Petitioner’s contentions for the remaining

limitations. On the present record, we determine that Petitioner has demonstrated sufficiently that each limitation of claim 14 is disclosed by the combination of Yarger and Love for the reasons that follow.

(i) *Preamble*

The preamble of claim 14 recites “A method for wireless communication of analyte data, the method comprising:” Ex. 1001, 116:58–59.

To the extent the preamble is limiting, Petitioner contends that Yarger discloses a method for wireless communication of analyte data, particularly glucose data, using a CGM system. Pet. 21. Specifically, Petitioner asserts that Yarger’s CGM system 100 comprises a glucose meter 105 and a glucose sensor 110 which communicate by a radio frequency (RF) wireless link. *Id.* (citing Ex. 1005, code (57), ¶¶ 1, 6, 16–17).

Patent Owner does not dispute Petitioner’s contention that Yarger discloses the preamble.

We find that Petitioner has shown sufficiently that the preamble of claim 14 is disclosed by Yarger, and thus do not reach the issue of whether the preamble is limiting.

(ii) *Limitation 14a: Measuring Analyte Values*

Limitation 14a recites “measuring analyte values in a host using a continuous analyte sensor of an analyte sensor system.” Ex. 1001, 116:60–61.

Petitioner contends that Yarger discloses this limitation by teaching a CGM system 100 comprising a glucose meter 105 and a glucose sensor 110, which measures and displays glucose level in a user’s body. Pet. 21–22 (citing Ex. 1005 ¶¶ 3, 17).

Patent Owner does not dispute Petitioner's contentions for limitation 14a.

On this record, we find that Petitioner shows sufficiently that Yarger discloses limitation 14a.

(iii) Limitation 14b: Using First Wireless Protocol

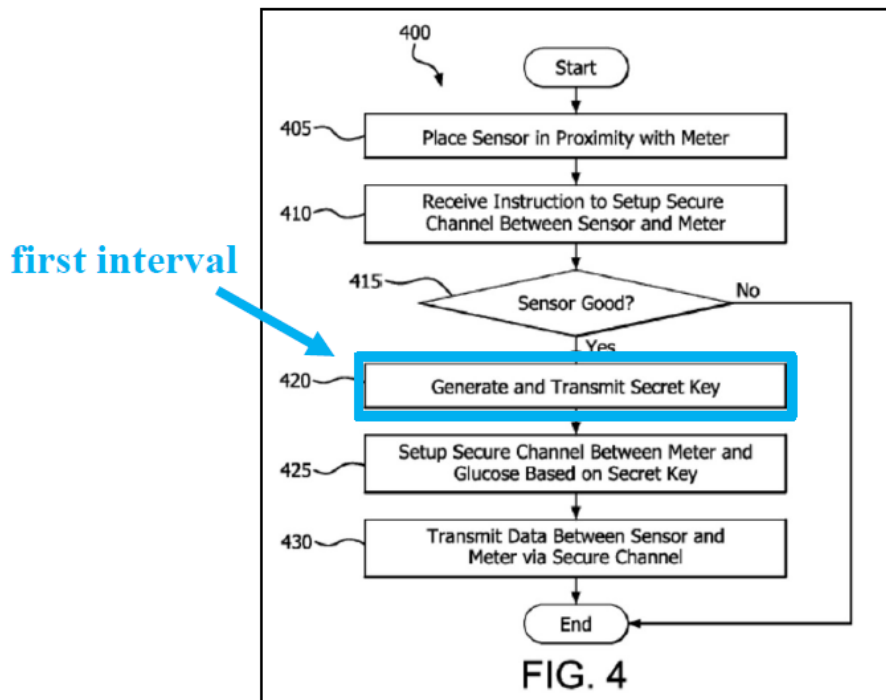
Limitation 14b recites “during a first interval, using a first wireless protocol to perform an exchange of information related to authentication with a display device.” Ex. 1001, 116:62–64.

(a) Petitioner's Contentions

Petitioner contends that “Yarger discloses using 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.” Pet. 22. Specifically, Petitioner asserts, “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).’” *Id.* at 22 (citing Ex. 1005 ¶¶ 14, 18, 22–23, 32–33, 35).

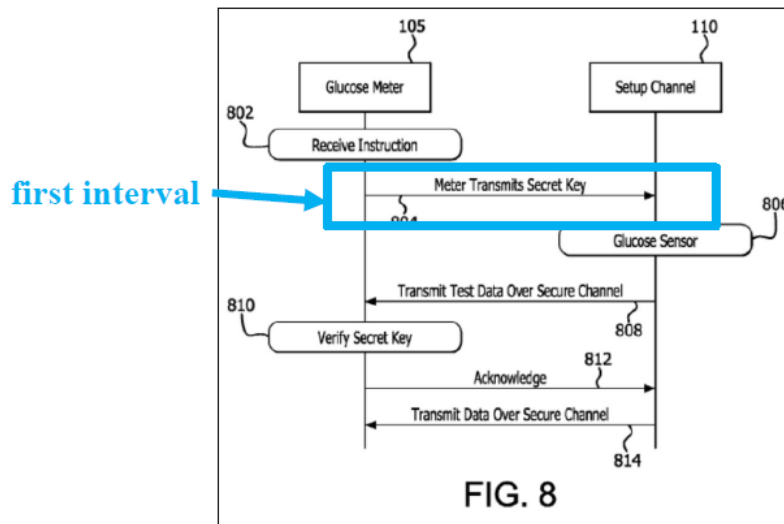
Petitioner argues that “Yarger discloses that its CGM meter device 105 comprises a display 120/214.” *Id.* at 22–23 (citing Ex. 1005 ¶¶ 17, 27, Figs. 1, 2 (annotated)).

Petitioner provides an annotated version of Yarger's Figure 4 as shown below.



Id. at 23. Petitioner annotates Figure 4 in blue to indicate that Step 420 labeled “Generate and Transmit Secret Key” occurs during the “first interval.” Petitioner contends that “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.” *Id.* (citing Ex. 1005 ¶ 35, Fig. 4).

Petitioner further provides an annotated version of Yarger’s Figure 8 as shown below.



Id. at 24. Petitioner annotates Yarger’s Figure 8 in blue to indicate that Step 804 labeled “Meter Transmits Secret Key” occurs during the “first interval.” Petitioner contends that Yarger’s Figure 8 “depicts an embodiment where the CGM meter (*i.e.*, the display device) transmits the secret key to the CGM sensor.” *Id.* at 23–24 (citing Ex. 1005 ¶¶ 46–47, Figs. 5–8). Petitioner states that “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.” *Id.* at 24–25 (citing Ex. 1005 ¶¶ 50–51).

Petitioner argues that “[t]he claimed ‘information related to authentication’ at least encompasses a random number related to identification of the sensor device or the display device.” *Id.* at 25 (citing *id.* § VI.A). Petitioner contends that “Yarger’s secret key can be a random number” and that “the initial ‘pairing’ operation involves an exchange of this secret key and ‘identifying information.’” *Id.* (citing Ex. 1005 ¶¶ 35, 51). “Accordingly,” Petitioner argues, “the exchange of the ‘secret key’ and ‘identifying information’ corresponds to the claimed ‘information related to

authentication.” *Id.* “Similarly,” Petitioner asserts, “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.’” *Id.* Petitioner further asserts that “Yarger’s NFC link used to exchange the secret key corresponds to the claimed ‘first wireless protocol.’” *Id.*

(b) Patent Owner’s Contentions

Patent Owner presents a series of arguments relating to Petitioner’s contention that Yarger’s secret key, or an exchange of challenge and hash values, satisfies the part of limitation 14b reciting “information related to authentication.” Prelim. Resp. 29–43. Patent Owner argues that Petitioner alleges that Yarger’s NFC pairing exchanges disclose “information relating to authentication” and that Petitioner fails to give meaning to the term “authentication.” *Id.* at 29–32. Relatedly, Patent Owner argues that Petitioner fails to establish that Yarger’s secret key is “information related to authentication” because Petitioner did not show that Yarger uses its secret key to validate that a device is authorized according to Patent Owner’s construction of “authentication involves validating authorization.” *Id.* at 33–37. Instead, Patent Owner argues, “Yarger uses the secret key exchanged between the sensor and display devices over Yarger’s NFC connection only to encrypt subsequent RF communications between the sensor and the display.” *Id.* at 37–38 (citing *id.* at § III.C; Ex. 1005 ¶¶ 18, 22, 36). Patent Owner further argues that Petitioner’s contention “hinges entirely on its improper claim construction” conflating “authentication” and “identification.” *Id.* at 38.

Patent Owner contends that Petitioner fails to establish that Yarger’s secret key meets Petitioner’s construction of “information related to authentication” because Yarger’s secret key is not “related to identification” of any device. *Id.* at 39–41. Patent Owner argues that Petitioner relies on a key in Yarger that is a random number and thus is not a unique identifier of a device. *Id.* at 40.

Accordingly, Patent Owner argues that Petitioner does not establish that Yarger’s secret key is used for any purpose other than to encrypt communications, and, unlike the ’222 patent, does not “perform authentication by validating that either Yarger’s sensor or display device is an authorized device.” *Id.* at 43.

Patent Owner’s next series of arguments relate to Petitioner’s contention that Yarger’s “identifying information” satisfies the part of limitation 14b reciting “information relating to authorization.” *Id.* at 43–49. Specifically, Patent Owner argues that Petitioner’s reliance on Yarger’s “identifying information” fails because it does not meet what Patent Owner alleges as Petitioner’s construction. *Id.* at 44. Patent Owner argues that Yarger discloses a pairing operation that allows devices to “exchange cryptographic key and **identifying information** that ensures that subsequent communication between the device 110 and 105 is secure.” *Id.* (citing Ex. 1005 ¶ 51). Patent Owner states that this is the only mention of “identifying information” in Yarger.

Patent Owner argues that Yarger does not explain what the “identifying information” is that is exchanged during the NFC “pairing operation.” *Id.* at 45 (citing Ex. 1005 ¶ 51). According to Patent Owner, “pairing” is mutual registering of identification information between two

devices that allows the devices to communicate, which is “akin to two people exchanging phone numbers.” *Id.* (citing Ex. 1009, 10). Patent Owner argues that “[p]airing by exchanging identifying information is not authentication because neither device validates the other device or determines whether the other device is authorized to do anything.” *Id.* (citing *id.* at § III.B).

Patent Owner further asserts that Yarger does not perform “authenticated pairing.” *Id.* at 45–49. Patent Owner argues that Petitioner “obfuscates by suggesting that Yarger’s use of NFC for pairing and setting up a Bluetooth link was understood in the art to be authentication.” *Id.* at 45–47 (citing Pet. 13). Patent Owner argues that the “authenticated pairing” described in Exhibit 1009 and Chivallier is different from the “simple pairing” described in Yarger, which allegedly is used only for encryption, not for authentication. *Id.* at 46–48 (citing Ex. 1008 ¶¶ 18, 20, 22, 28–29, 36; Ex. 1009, 7).

Patent Owner further contends that Petitioner fails to establish that Yarger’s secret key and identifying information together constitute “information related to authentication.” *Id.* at 49. Patent Owner reiterates its assertion that “neither Yarger’s secret key nor its identifying information has anything to do with authentication.” Prelim. Resp. 49 (citing *id.* at §§ III.D.3–4; Pet. 25). Patent Owner argues that “[n]either Yarger’s sensor nor its display device authenticates the other” and asserts that Yarger’s short-range NFC and inductive coupling ensures only authorized devices are paired. *Id.* (citing § III.C; Ex. 1005 ¶ 51). Patent Owner argues that Petitioner “fails to establish that Yarger’s devices exchange any ‘information related to authentication.’” *Id.*

Furthermore, Patent Owner argues that Petitioner’s expert “testimony parrots *verbatim* the Petition’s argument.” *Id.* at 50 (citing Pet. 25; Ex. 1003 ¶ 82) (emphasis original). Patent Owner contends that Petitioner’s expert “testimony warrants no weight under the Board’s precedential *Xerox* decision because it repeats the Petition’s arguments word-for-word without providing any meaningful analysis or corroborating evidence.” *Id.* (citing *Xerox v. Bytemark*, IPR2022-00624, Paper 9, 15 (Aug. 24, 2022) (precedential)). Patent Owner asserts that “the cited expert testimony adds nothing to [Petitioner’s] argument” and “is unsupported by Yarger or any other evidence supporting the assertion that the information Yarger exchanges during its NFC pairing is ‘information related to authentication’ as claimed.” *Id.* at 50–51. Patent Owner concludes that “the Petitioner fails to establish that its alleged Yarger-Love combination meets exchanging ‘information related to authentication’” as claimed. *Id.* at 51.

(c) *Discussion*

Patent Owner’s arguments hinge critically on the incorrect constructions that it advances, or that it alleges that Petitioner advances. Prelim. Resp. 29–49. Specifically, Patent Owner contends that “authentication involves validating authorization” and that Petitioner’s construction equates “authentication” with “identification.”

Because the claim terms “authentication” and “identification” were well-known and understood in the art, we reject Patent Owner’s construction arguments, and instead apply the ordinary and customary meaning of these terms. Thus, Patent Owner’s construction-related arguments do not undermine Petitioner’s contentions. *See* § III.C.

Turning to Patent Owner’s argument that Yarger does not disclose the claimed “information related to authentication,” we note that Patent Owner does not dispute that Yarger’s secret keys, challenges, hashes, and identifying information would have been understood to be useful to perform authentication. Nor does Patent Owner dispute that “authenticated pairing” was known in the art. Ex. 1009, 7; Ex. 1008. Instead, Patent Owner’s argument is that Yarger does not expressly disclose that its secret keys, challenges and responsive hashes, or identifying information, are used for authentication.

For limitation 14h, however, Petitioner cites to a portion of Love disclosing a sensor control device that transmits a digital signature to a reader device. Pet. 34–36 (citing Ex. 1006 ¶¶ 151–155, Fig. 8B). The digital signature is generated using a private key, the assigned serial number of the sensor control device, and a random number. Ex. 1006 ¶ 150. The reader device uses a public key to extract the serial number of the sensor device and a random number contained therein. *Id.* ¶ 151. The reader device can itself check the serial number against a local compilation of serial numbers that indicates whether the serial numbers are already in use or are counterfeit, or a trusted computer system may perform this check. *Id.* ¶ 155. Love expressly discloses that this check is part of an “authentication” process. *Id.*

Hence, Love’s private key, serial number, and random number would be viewed as “information related to authentication” as claimed, as Love expressly discloses. *Id.* Viewed in light of Love and the fact that “authenticated pairing” was known in the art, Yarger’s secret keys, challenges and responsive hashes, and identifying information also would

have been viewed as “information related to authentication.” The term “identifying information” in Yarger would have been understood to encompass Love’s serial number. Although Petitioner does not mention Love in connection with limitation 14b, viewing the Petition as a whole, Petitioner’s showing is sufficient for institution.

Patent Owner argues that we should accord “no weight” to Petitioner’s expert declaration because it “parrots” the Petition. Prelim. Resp. 50. Although there is common language in the Petition and Dr. Kiaei’s declaration (Pet. 25; Ex. 1003 ¶ 82), Patent Owner’s argument overlooks that these statements are supported by corroborating evidence in Yarger (Ex. 1005 ¶¶ 35, 51) as well as the background that Dr. Kiaei provided in the preceding paragraph (Ex. 1003 ¶ 81) of the declaration. Thus, we decline to take the extreme view of according “no weight” as Patent Owner proposes, and decide for ourselves the appropriate weight to give the testimony in light of the support provided.

On the current record, after reviewing the arguments and evidence, we find that Petitioner shows sufficiently that limitation 14b is disclosed by the combination of Yarger and Love.

(iv) Limitation 14c: Determination for Triggering Alert

Limitation 14c recites “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.” Ex. 1001, 116:65–67.

Petitioner contends that the combination of Yarger and Love discloses limitation 14c. Pet. 25–27. Specifically, Petitioner contends that “Yarger discloses that its CGM system is used for monitoring ‘physiological conditions,’ i.e., medical conditions, as part of a ‘diabetes management

system.” *Id.* at 25–26 (citing Ex. 1005, code (57), ¶¶ 1, 53). Petitioner asserts that “[w]hile 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.” *Id.* at 26–27 (citing Ex. 1006 ¶¶ 63, 70, 78, 98, Fig. 1). Petitioner alleges that “[i]n 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.” *Id.* at 27.

Patent Owner does not dispute Petitioner’s contentions for limitation 14c.

On this record, we find that Petitioner shows sufficiently that limitation 14c is disclosed by the combination of Yarger and Love.

(v) *Limitation 14d: Triggering Alert and Providing Notification*

Limitation 14d recites “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.” Ex. 1001, 117:1–4.

Petitioner contends that the combination of Yarger and Love discloses limitation 14d. Pet. 27–28. Specifically, Petitioner contends that “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.” *Id.* at 27 (citing Ex. 1006 ¶¶ 70, 78, 98) (emphases original).

Petitioner asserts that “[i]n 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.” *Id.* at 27–28.

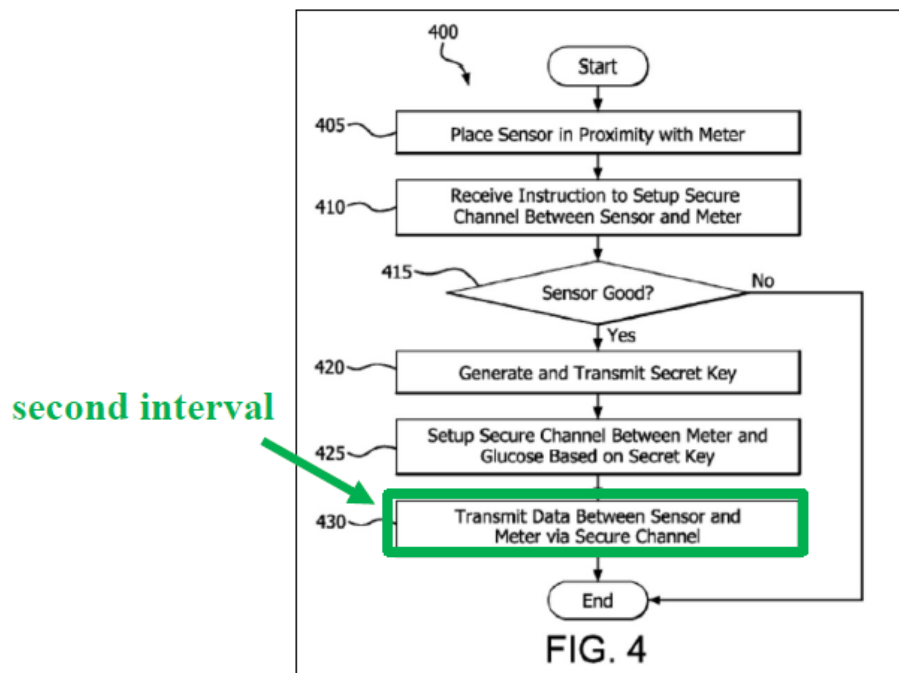
Patent Owner does not dispute Petitioner’s contentions for limitation 14d.

On the present record, we find that Petitioner shows sufficiently that the combination of Yarger and Love discloses limitation 14d.

(vi) *Limitation 14e: Using Second Wireless Protocol*

Limitation 14e recites “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.” Ex. 1001, 117:5–8.

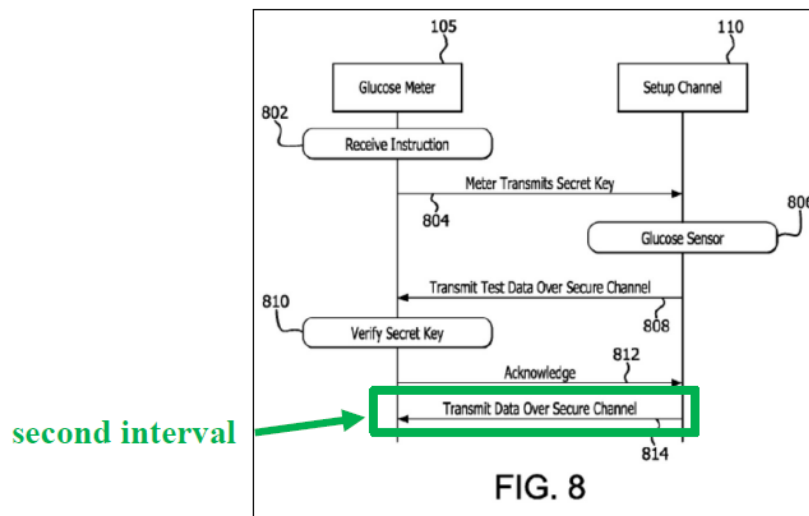
Petitioner contends that Yarger discloses limitation 14e. Pet. 28–30. Specifically, Petitioner asserts that “Yarger discloses bypassing the exchange of the secret key and identifying information (i.e., the information related to authentication) during a second interval by using a second wireless protocol (i.e., Bluetooth, ZigBee, or other wireless protocol) to transmit an encrypted analyte value to a display device.” *Id.* at 28 (citing Ex. 1005, code (57), ¶ 14). Petitioner provides the following annotated version of Yarger’s Figure 4.



Id. at 29. Petitioner annotates Yarger’s Figure 4 above in green to indicate that Step 430 labeled “Transmit Data Between Sensor and Meter via Secure Channel” occurs during the second interval.

Petitioner quotes Yarger as stating that “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)*” and “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” which the receiving device decrypts using the secret key. *Id.* (citing Ex. 1005 ¶¶ 36–37, Fig. 4) (emphases original).

Petitioner also provides an annotated version of Yarger’s Figure 8 as shown below.



Id. at 30. Petitioner annotates Yarger’s Figure 8 above in green to indicate that Step 814 labeled “Transmit Data Over Secure Channel” occurs during the “second interval.” *Id.*

Petitioner contends that “[t]he 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.’” Pet. 30. Similarly, Petitioner contends, “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.’” *Id.* at 30.

Furthermore, Petitioner contends, “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.’” *Id.* (citing Ex. 1005 ¶ 35).

Patent Owner does not dispute Petitioner’s contention that Yarger discloses limitation 14e.

On the current record, we find that Petitioner demonstrates sufficiently that Yarger discloses limitation 14e.

(vii) Limitation 14f: Encrypted Analyte Value

Limitation 14f recites “wherein the encrypted analyte value has been generated using the information related to authentication.” Ex. 1001, 117:8–10.

Petitioner contends that Yarger discloses limitation 14f. Pet. 31. According to Petitioner, “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’” *Id.* (citing Ex. 1005 ¶¶ 16, 36 (“the glucose meter and glucose sensor transmit data over the wireless channel that is encrypted . . . using the secret key.”)) (alterations in original).

Patent Owner does not dispute Petitioner’s contention that Yarger discloses limitation 14f.

On the current record, we find that Petitioner demonstrates sufficiently that Yarger discloses limitation 14f.

(viii) Limitation 14g: Different Wireless Protocols

Limitation 14g recites “wherein the first wireless protocol is different than the second wireless protocol.” Ex. 1001, 117:10–11.

Petitioner contends that “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.). Pet. 31 (citing Ex. 1005 ¶¶ 16, 18, 36).

Patent Owner does not dispute Petitioner's contention that Yarger discloses limitation 14g.

On the current record, we find that Petitioner demonstrates sufficiently that Yarger discloses limitation 14g.

(ix) *Limitation 14h: Neither Initiating Transmission Nor Providing Notification*

Limitation 14h recites “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.” Ex. 1001, 117:12–15.

Petitioner contends that the combination of Yarger and Love discloses limitation 14h. Pet. 31–36. Specifically, Petitioner contends that “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.” *Id.* at 31–32. Petitioner contends “[f]or example, Yarger requires the secret key to be exchanged before the secure channel can be setup.” *Id.* at 32 (citing Ex. 1005 ¶ 36 (“After both the glucose meter and the glucose sensor have identical secret keys, the glucose sensor and glucose meter setup a secure wireless channel”); ¶¶ 39–47 (“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”), Figs. 4–8).

Petitioner further argues that “[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.” *Id.* at 34 (citing Ex. 1003 ¶ 101).

Petitioner contends that “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.” *Id.* Petitioner asserts that “[a]s 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.” *Id.* at 34–36 (citing Ex. 1006 ¶¶ 151–155, Fig. 8B). Thus, Petitioner argues, “Love discloses that the glucose data is not transmitted if the information related to authentication was not successfully exchanged.” *Id.* at 36 (citing Ex. 1003 ¶¶ 102–103). Because Love generates alarms and alerts based on current analyte levels, Petitioner contends that 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. *Id.*

Petitioner asserts that “[a]ccordingly, 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.” *Id.* (citing Ex. 1003 ¶ 104).

Patent Owner does not dispute Petitioner's contentions for limitation 14h.

On the present record, we find that Petitioner shows sufficiently that the combination of Yarger and Love discloses limitation 14h.

(x) Conclusion for Claim 14

Petitioner has shown sufficiently on this record that a POSITA would have had reason to combine Yarger and Love with a reasonable expectation of success, and that each limitation of claim 14 is disclosed by the combination.

Accordingly, we determine that Petitioner has demonstrated a reasonable likelihood to prevail in demonstrating unpatentability of claim 14 of the '222 patent as obvious over the combination of Yarger and Love.

5. Claim 15

Claim 15 depends from claim 14 and recites "[15a] 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 [15b] wherein the second wireless protocol is selected from a group consisting of: WiFi communication, NFC and BLE communication." Ex. 1001, 117:16–21.

(i) Limitation 15a: First Wireless Protocol

Petitioner contends that "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).'" Pet. 37 (citing Ex. 1005 ¶¶ 18, 23, 26, 29, 50, Figs. 2–3 (annotated)) (emphasis omitted).

Patent Owner does not dispute Petitioner's contentions for limitation 15a.

On this record, we find that Petitioner shows sufficiently that Yarger discloses limitation 15a.

(ii) Limitation 15b: Second Wireless Protocol

Petitioner contends that "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)." Pet. 38 (citing Ex. 1005 ¶¶ 31, 36, Figs. 2–3 (annotated)).

Patent Owner does not dispute Petitioner's contentions for limitation 15b.

On the present record, we find that Petitioner shows sufficiently that Yarger discloses limitation 15b.

(iii) Conclusion for Claim 15

On the current record, Petitioner presents a reasonable likelihood of to prevail in demonstrating unpatentability of claim 15 of the '222 patent as obvious over the combination of Yarger and Love.

6. Claim 16

Claim 16 depends from claim 14 and recites "[16a] wherein the analyte sensor system is a continuous glucose sensor system and [16b] the information related to authentication comprises an application key."

(i) Limitation 16a: Continuous Glucose System

Petitioner contends that Yarger discloses a CGM system. Pet. 39. Specifically, Petitioner notes that Yarger states that "[a] physiological

condition monitoring system (e.g., a continuous glucose monitoring system) includes a physiological condition meter and a physiological condition sensor.” *Id.* (citing Ex. 1005 code (57), ¶¶ 1, 14, 53) (emphasis omitted).

Patent Owner does not dispute Petitioner’s contentions for limitation 16a.

On this record, we find that Petitioner shows sufficiently that Yarger discloses limitation 16a.

(ii) *Limitation 16b: Application Key*

Petitioner contends that Yarger discloses that during initial pairing 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.” Pet. 39. Petitioner asserts that “the claimed ‘application key’ at least encompasses a random number.” *Id.* Petitioner argues that “Yarger discloses the information related to authentication comprises an application key.” *Id.*

Patent Owner does not dispute Petitioner’s contentions that Yarger discloses limitation 16b.

On the current record, Petitioner shows sufficiently that Yarger discloses limitation 16b.

(iii) *Conclusion for Claim 16*

Petitioner demonstrates a reasonable likelihood to prevail in demonstrating claim 16 would have been obvious over the combination of Yarger and Love.

7. *Claim 18*

Petitioner asserts that the combination of Yarger and Love renders claim 18 obvious. Pet. 39–43 (citing Ex. 1003 ¶¶ 115–138). Patent Owner

disputes Petitioner's contentions with the same arguments that it presented for claim 14. Prelim. Resp. 16–51. We consider Petitioner's and Patent Owner's contentions for each limitation of claim 18.

(i) *Preamble*

The preamble of claim 18 recites “An analyte sensor system configured for wireless communication of analyte data, the analyte sensor system comprising.” Ex. 1001, 117:28–30.

Petitioner contends that “[t]o the extent the preamble is limiting, Yarger discloses a system for wireless communication of analyte data” for the same reasons stated for claim 14's preamble. Pet. 39.

Patent Owner does not dispute Petitioner's contentions regarding the preamble.

On the current record, we find that Petitioner shows sufficiently that the preamble of claim 18 is disclosed by Yarger. Consequently, we do not decide whether the preamble is limiting.

(ii) *Limitation 18a: Sensor*

Limitation 18a recites “a continuous analyte sensor configured to measure analyte values in a host.” Ex. 1001, 117:31–32.

Petitioner contends that Yarger discloses limitation 18a for the same reasons stated for limitation 14a. Pet. 40.

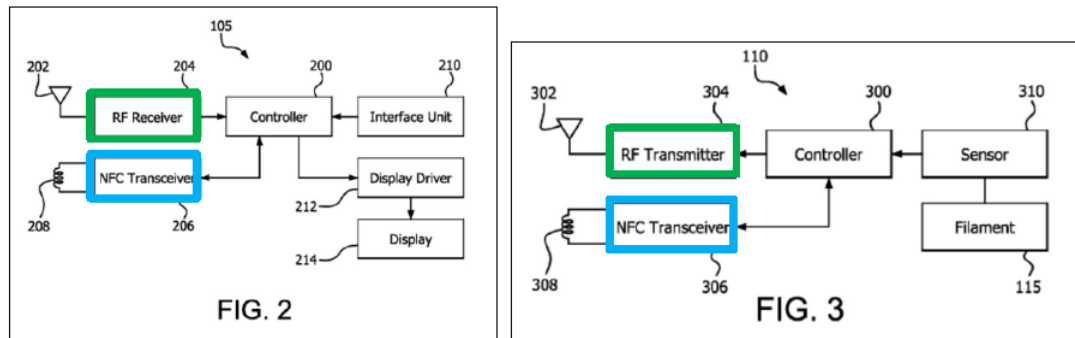
Patent Owner does not dispute Petitioner's contention.

On the current record, we find that Petitioner shows sufficiently that Yarger discloses limitation 18a.

(iii) *Limitation 18b: Transceiver*

Limitation 18b recites “a transceiver configured to transmit and receive wireless signals.” Ex. 1001, 117:33–34.

To explain its contentions for limitation 18b, Petitioner provides annotated versions of Yarger's Figures 2 and 3 as shown below.



Petitioner contends that Yarger discloses that both the CGM meter (Figure 2 above) and CGM sensor (Figure 3 above) contain multiple transceivers configured to transmit and receive wireless signals, including NFC transceivers (annotated in blue) for exchanging a secret key, and separate RF transceivers for communicating encrypted analyte data (annotated in green). Pet. 40 (citing Ex. 1005 ¶¶ 25–31). Petitioner notes that “[w]hile 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.* (citing Ex. 1005 ¶ 31) (alteration in original).

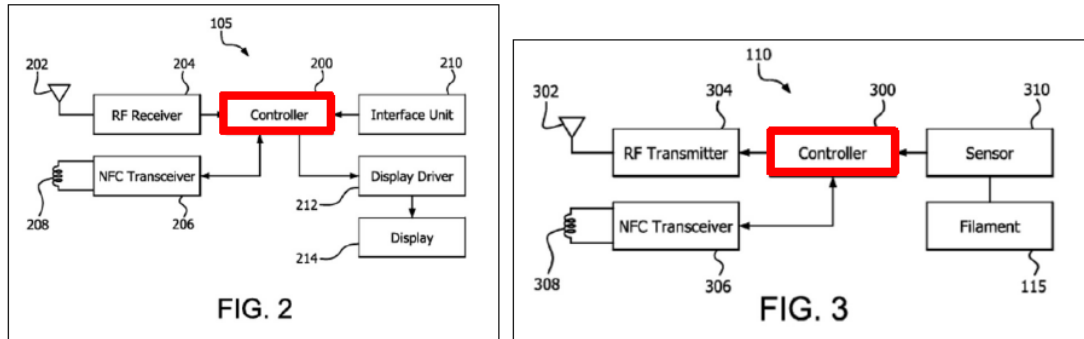
Patent Owner does not dispute Petitioner's contentions concerning limitation 18b.

On this record, we find that Petitioner shows sufficiently that Yarger discloses limitation 18b.

(iv) *Limitation 18c: Processor*

Limitation 18c recites “a processor operatively coupled to the analyte sensor and the transceiver and configured to cause the analyte sensor system to:” Ex. 1001, 117:35–37.

To explain its contentions for limitation 18c, Petitioner provides annotated versions of Yarger's Figures 2 and 3 as shown below.



Pet. 41. Petitioner contends that Yarger discloses that both the CGM meter (Figure 2) and the CGM sensor (Figure 3) contain controllers (annotated above in red) operably coupled to the analyte sensor and transceivers, and discloses that these controllers may be, for example, microprocessors. *Id.* (citing Ex. 1005 ¶¶ 25–31). According to Petitioner, “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.* (citing Ex. 1005 ¶¶ 25–27). Petitioner further asserts that “[s]imilarly, 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.* (citing Ex. 1005 ¶¶ 28–30). Petitioner argues that “[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” for limitations 18d–18j. *Id.* at 41–42 (citing Ex. 1003 ¶ 124).

Patent Owner does not dispute Petitioner’s contentions for limitation 18c.

On the current record, we find that Petitioner shows sufficiently that Yarger discloses limitation 18c.

(v) *Limitation 18d: Establishing First Connection*

Limitation 18d recites “during a first interval, establish a first connection between the analyte sensor system and a display device.” Ex. 1001, 117:38–40.

As explained for limitation 14b, Petitioner asserts that “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.” Pet. 42. Petitioner contends that “[t]he NFC connection corresponds to the ‘first connection.’” *Id.*

Patent Owner does not dispute Petitioner’s contentions concerning limitation 18d.

On the current record, we find that Petitioner shows sufficiently that limitation 18d is disclosed by Yarger.

(vi) *Limitation 18e: Exchange Information Related to Authentication*

Limitation 18e recites “during the first connection, exchange information related to authentication between the analyte sensor system and the display device.” Ex. 1001, 118:1–3.

Petitioner contends that, as explained for limitation 14b, “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.” Pet. 42.

Patent Owner does not dispute Petitioner's contentions for limitation 18e.

On the current record, we find that Petitioner shows sufficiently that limitation 18e is disclosed by the combination of Yarger and Love.

(vii) *Limitation 18f: First Determination*

Limitation 18f recites to “perform a first determination whether authentication was performed during the first interval.” Ex. 1001, 118:4–5.

Petitioner contends that, as explained for limitation 14h, “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.” Pet. 42. Petitioner asserts that “[t]he determination of whether the secret key was successfully exchanged corresponds to the ‘first determination whether authentication was performed during the first interval.’” *Id.*

Patent Owner argues that Petitioner erroneously equates verifying the exchange of a secret key as authentication. Prelim. Resp. 42. Patent Owner asserts that there is no evidence that verifying successful exchange of the secret key is authentication, and argues that such verification “does not authenticate anything.” *Id.*

As we explained for limitation 14b (*see* § III.D.4.iii.c, *supra*), Petitioner cited to portions of Love for limitation 14h that describe the use of a secret key, serial number, and random number to generate a digital signature exchanged between a sensor system and reader device to perform authentication. Pet. 34–36 (citing Ex. 1006 ¶¶ 151–155). In addition, viewed in light of Love and the fact that “authenticated pairing” was known, we find on this record that a POSITA would have viewed Yarger's secret

keys, challenges and responsive hashes, and identifying information as useful for authentication.

Thus, on the current record, we find that Petitioner shows sufficiently for institution that limitation 18f is disclosed by the combination of Yarger and Love.

(viii) Limitation 18g: Second Determination

Limitation 18g recites “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.” Ex. 1001, 118:6–8.

Petitioner asserts that limitation 18g is disclosed by the combination of Yarger and Love for the reasons stated for limitation 14c.

Patent Owner does not dispute Petitioner’s contentions for limitation 18g.

On this record, we find that Petitioner shows sufficiently that limitation 18g is disclosed by the combination of Yarger and Love.

(ix) Limitation 18h: Trigger Alert and Provide Notification

Limitation 18h recites “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 [be] triggered indicative of the medical condition of the host.” Ex. 1001, 118:9–12.

Petitioner asserts that limitation 18h is disclosed by the combination of Yarger and Love for the reasons stated for limitation 14d.

Patent Owner does not dispute Petitioner’s contentions for limitation 18h.

On this record, we find that Petitioner shows sufficiently that limitation 18h is disclosed by the combination of Yarger and Love.

(x) Limitation 18i: Transmit Encrypted Analyte Value

Limitation 18i recites “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.” Ex. 1001, 118:13–16.

Petitioner asserts that limitation 18i is disclosed by the combination of Yarger and Love for the reasons stated for limitation 14e.

Patent Owner does not dispute Petitioner’s contentions for limitation 18i.

On the current record, we find that Petitioner shows sufficiently that limitation 18i is disclosed by Yarger.

(xi) Limitation 18j: Neither Initiate Transmission Nor Provide Notification

Limitation 18j recites “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.” Ex. 1001, 118:16–21.

Petitioner asserts that limitation 18j is disclosed by the combination of Yarger and Love for the reasons stated for limitation 14h.

Patent Owner does not dispute Petitioner’s contentions for limitation 18j.

On the current record, we find that Petitioner shows sufficiently that limitation 18j is disclosed by the combination of Yarger and Love.

(xii) Conclusion for Claim 18

On the current record, we determine that Petitioner shows sufficiently that a POSITA would have been motivated to combine Yarger and Love with a reasonable expectation of success. *See* § III.D.3, *supra*. We further

find that Petitioner shows that each limitation of claim 18 is disclosed by the combination of Yarger and Love. Accordingly, we determine that Petitioner presents a reasonable likelihood to prevail in demonstrating unpatentability of claim 18 as obvious over the combination of Yarger and Love.

8. *Claim 19*

Claim 19 depends from claim 18 and recites “[19a] 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 [19b] during the second connection, bypass the exchange of the information related to authentication.” Ex. 1001, 118:22–29.

(i) *Limitation 19a: Second Connection*

Petitioner contends that the combination of Yarger and Love renders claim 19 obvious. Pet. 43 (citing Ex. 1003 ¶¶ 139–143). Specifically, Petitioner contends, as explained for limitation 14e, “Yarger discloses using a second wireless protocol (e.g., BLE, Wi-Fi, ZigBee) to communicate the encrypted analyte data during a second interval.” *Id.* at 44. Petitioner contends that “[t]he RF connection (whether BLE, Wi-Fi, ZigBee, or other protocol) corresponds to the ‘second connection.’” *Id.*

Patent Owner does not dispute Petitioner’s contentions for limitation 19a.

On the current record, we find that Petitioner shows sufficiently that limitation 19a is disclosed by Yarger.

(ii) *Limitation 19b: Bypass Exchange of Information Related to Authentication*

Petitioner asserts that limitation 19b is disclosed by the combination of Yarger and Love for the reasons stated for limitation 14e.

Patent Owner does not dispute Petitioner's contentions for limitation 19b.

On this record, we find that Petitioner shows sufficiently that limitation 19b is disclosed by the combination of Yarger and Love.

(iii) Conclusion for Claim 19

On the current record, Petitioner presents a reasonable likelihood to prevail in demonstrating unpatentability of claim 19 as obvious over the combination of Yarger and Love.

9. Claim 20

Claim 20 depends from claim 19 and recites

[20a] wherein the analyte sensor system is a continuous glucose sensor system, and [20b] the information related to authentication comprises an application key [20c] 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 [20d] wherein the use of the application key allows the analyte sensor system to bypass the exchange.

Ex. 1001, 118:30–39.

(i) Limitation 20a: Continuous Glucose Sensor System

Petitioner contends that Yarger discloses limitation 20a for the reasons stated in the Petition for limitation 16a. Pet. 44.

Patent Owner does not dispute Petitioner's contention that Yarger discloses limitation 20a.

On this record, Petitioner shows sufficiently that Yarger discloses limitation 20a.

(ii) Limitation 20b: Application Key

Petitioner contends that Yarger discloses limitation 20b for the reasons stated in the Petition for limitation 16b. Pet. 44.

Patent Owner does not dispute Petitioner's contention that Yarger discloses limitation 20b.

On this record, Petitioner shows sufficiently that Yarger discloses limitation 20b.

(iii) Limitation 20c: Processor

Petitioner contends that "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," as explained in the Petitioner for limitation 14f. Pet. 44–45.

Patent Owner does not dispute Petitioner's contentions that Yarger discloses limitation 20c.

On this record, Petitioner shows sufficiently that Yarger discloses limitation 20c.

(iv) Limitation 20d: Application Key Allows Bypass

Petitioner contends that Yarger discloses limitation 20d for the reasons stated in the Petition for limitation 14e. Pet. 45.

Patent Owner does not dispute Petitioner's contentions that Yarger discloses limitation 20d.

On this record, Petitioner shows sufficiently that Yarger discloses limitation 20d.

(v) *Conclusion for Claim 20*

On the current record, Petitioner presents a reasonable likelihood to prevail in demonstrating unpatentability of claim 20 as obvious over the combination of Yarger and Love.

E. Ground 2: Obviousness over Hernandez-Rosas and Chivallier

Petitioner asserts that claims 14–16 and 18–20 of the '222 patent would have been obvious over the combination of Hernandez-Rosas and Chivallier. Pet. 45–83. Patent Owner disagrees. Prelim. Resp. 58–72.

We conclude that the record demonstrates a reasonable likelihood that Petitioner would prevail with respect to challenged claims 14–15 and 18–19, but not claims 16 and 20, for the following reasons.

1. Hernandez-Rosas (Ex. 1007)

Hernandez-Rosas is titled “Systems and Methods for Continuous Monitoring of Analyte Values.” Ex. 1007, code (54). Hernandez-Rosas discloses wireless data communication between an analyte sensor system and a mobile device. *Id.*, code (57). A user enters identification information associated with a transceiver of the analyte sensor system via a custom application running on the mobile device. *Id.* The mobile device receives an advertisement signal from the transceiver and authenticates it using the identification information. *Id.* The custom application requests confirmation from the user that data connection with the transceiver is desired and, if the user confirms the connection, completes data connection with the transceiver. *Id.*

Hernandez-Rosas’s Figure 4 is shown below.

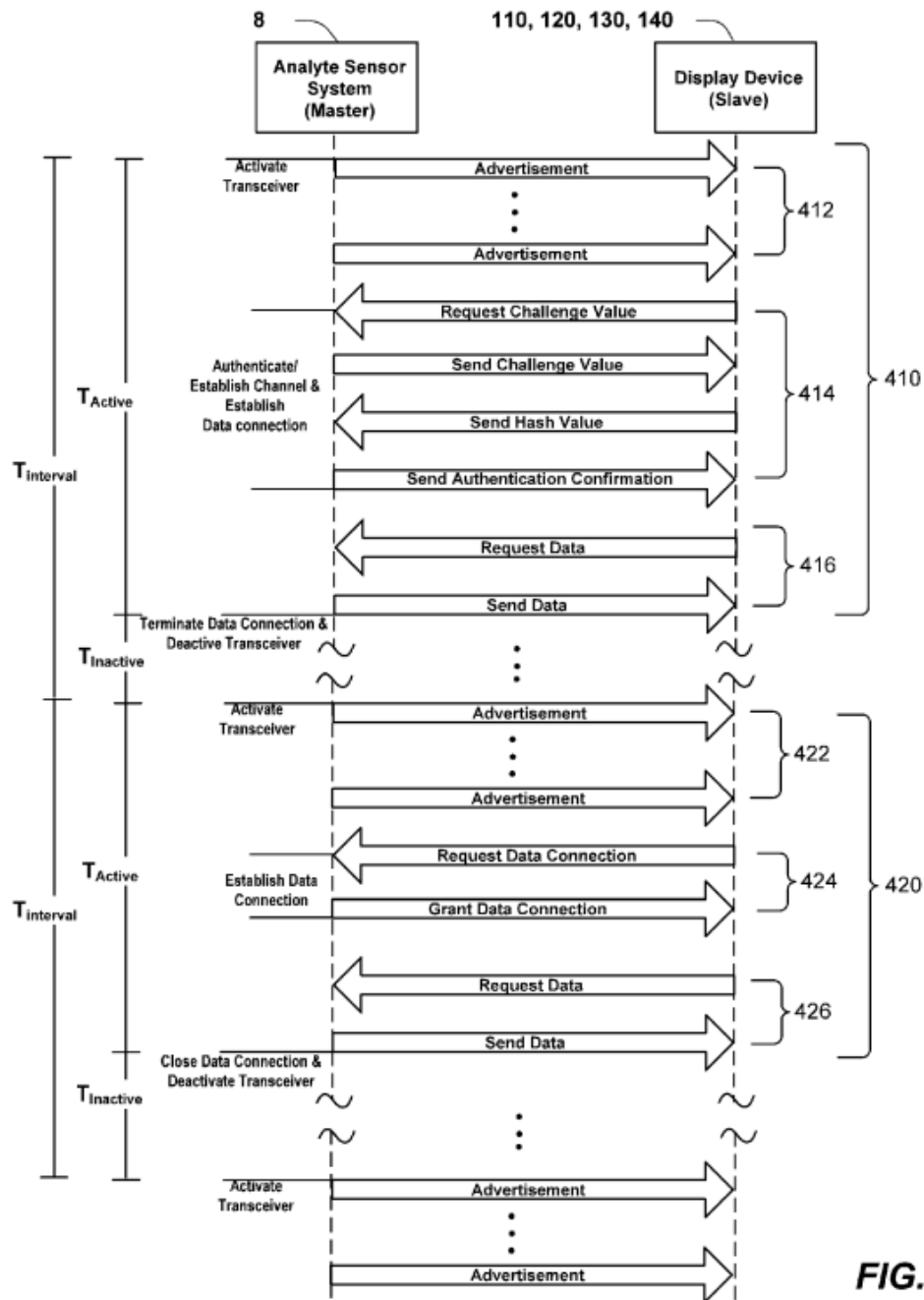


FIG. 4

Hernandez-Rosas’s Figure 4 above shows a wireless data communication procedure between analyte sensor system and a display device capable of receiving analyte data values from the analyte sensor system. *Id.* ¶ 94. Data connection process 414 labeled “Authenticate/Establish Channel & Establish Data Connection” involves exchange of challenge request, challenge, hash,

and confirmation between analyte sensor system 8 and display devices 110, 120, 130, 140. *Id.* ¶ 150, Fig. 4.

Hernandez-Rosas also discloses that alerts may be transmitted from the analyte sensor system to a display device to apprise that the host has a hypoglycemic condition. *Id.* ¶¶ 106–107.

2. *Chivallier (Ex. 1008)*

Chivallier is titled “Data Transmission of Sensors.” Ex. 1008, code (54). Chivallier is directed to a method for data transmission between a sensor module and a mobile device. *Id.*, code (57). The sensor module and mobile device are authenticated to each other by comparing respective security keys, after which the sensor module and mobile device are paired for secure data transmission. *Id.* The sensor module may use a wireless connection to communicate with the mobile device using NFC or other wireless protocols. *Id.* ¶¶ 16–17. Chivallier further discloses that “the bio-sensor can effectively provide an alert if the analysis provides a critical result for the health of the patient.” *Id.* ¶ 2.

3. *Motivation to Combine with Reasonable Expectation of Success*

We now address Petitioner’s contentions regarding the motivation to combine Hernandez-Rosas and Chivallier with a reasonable expectation of success, and Patent Owner’s arguments against the combination. Pet. 45–48; Prelim. Resp. 58–72.

(i) *Petitioner’s Contentions*

Petitioner contends that Hernandez-Rosas discloses an authentication procedure to secure communication of glucose data between a sensor device and display device. Pet. 45–46 (citing Ex. 1007, code (57)). Petitioner quotes Hernandez-Rosas as stating that authentication is “required for

communication between the sensor electronics module and the display device.” *Id.* at 46 (citing Ex. 1007 ¶ 119). Petitioner contends that “[a] POSITA would have understood that a successful authentication and encryption scheme would prevent an eavesdropper or man-in-the-middle from determining the encryption key, otherwise an unauthorized device might be able to mimic the authentication steps.” *Id.* (citing Ex. 1003 ¶¶ 154–155). Petitioner asserts that “[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.” *Id.* (citing Ex. 1003 ¶ 155).

Petitioner contends that “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.” *Id.* (citing Ex. 1008, code (57), ¶¶ 4–5). Petitioner asserts Chivallier discloses bringing a mobile phone in “close proximity” with a sensor device to initiate the authentication process by transmitting a private key from sensor device to mobile device via an NFC link. *Id.* (citing Ex. 1008 ¶¶ 17–20, 28). Petitioner asserts that “Chivallier’s mobile device then uses a public key corresponding to the sensor’s private key to recognize and authenticate the sensor.” *Id.* (citing Ex. 1008 ¶ 29).

Petitioner alleges that “[a]fter 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 47 (citing Ex. 1008 ¶¶ 16, 30–31). Petitioner asserts that “[a] POSITA would have

understood that the range of an NFC communication is on the order of a few centimeters” and that using Chivallier’s NFC link “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.” *Id.* (citing Ex. 1003 ¶¶ 33, 157).

Petitioner contends that a POSITA would have been motivated to use Chivallier’s short-range NFC link to exchange information related to authentication in Hernandez-Rosas’s CGM system to achieve its stated goal of preventing eavesdropping. *Id.* (citing Ex. 1003 ¶¶ 158–161). Petitioner asserts that a POSITA would have had a reasonable expectation of success in using Chivallier’s NFC transmitters and receivers in Hernandez-Rosas’s CGM system because they were well-known and it would have been within a POSITA’s skill to incorporate them with Hernandez-Rosas’s CGM system. *Id.* at 47–48 (citing Ex. 1003 ¶ 162; Ex. 1005, Figs. 2, 3; Ex. 1008, Fig. 2).

Petitioner also states that Hernandez-Rosas and Chivallier are analogous art because they both relate to securely authenticating a sensor device and display device, and securely communicating sensor measurements over wireless links. *Id.* at 48 (citing Ex. 1007, code (57); Ex. 1008, code (57); Ex. 1003 ¶ 158).

(ii) *Patent Owner’s Contentions*

Patent Owner argues that Hernandez-Rosas’s CGM system is immune to the eavesdropping and mimicking that Petitioner alleges it has, so a POSITA would not have been motivated to use Chivallier’s NFC in its CGM system. Prelim. Resp. 59, 61–66. Specifically, Patent Owner asserts that Hernandez-Rosas’s authentication requires a challenge, sensor identification information, a hash function, and the knowledge to use them to calculate a

valid hash value. *Id.* at 61–62 (citing Ex. 1007 ¶¶ 149–150). Patent Owner argues Petitioner fails to identify any information exchanged during Hernandez-Rosas’s authentication that would create a risk of unauthorized access if intercepted by an eavesdropper, or how such exchanged information could be mimicked as Petitioner contends. *Id.* at 62–66 (citing Pet. 46–47; Ex. 1007 ¶¶ 19, 149–150; Ex. 2005, 7, 10–11, 54, 73).

Patent Owner further argues that Petitioner fails to explain the contemplated working of the combination. *Id.* at 66–68. Patent Owner argues that Chivallier uses a passive NFC tag on the sensor which is read by an NFC reader on the mobile device to obtain the sensor’s private key stored therein. *Id.* at 66–67 (citing Ex. 1007 ¶¶ 17, 20; Ex. 1003 ¶ 161). According to Patent Owner, Hernandez-Rosas’s authentication process is a multi-step challenge-response process that requires that both sensor and display devices are capable of receiving and processing information. *Id.* at 67. Patent Owner argues that Petitioner did not explain how Chivallier’s passive NFC tag would have worked in Hernandez-Rosas’s multi-step authentication process which requires both devices to receive and process information. *Id.* at 67–68.

In addition, Patent Owner argues that Petitioner ignores reasons why a POSITA would not have used Chivallier’s passive NFC tag and NFC reader to exchange Hernandez-Rosas’s authentication information. *Id.* at 68–71. Specifically, Patent Owner argues that Hernandez-Rosas’s four-step challenge-response authentication is incompatible with the NFC that Chivallier uses for its simple one-step private key sharing. *Id.* at 68–70 (citing Ex. 1007 ¶ 150, Fig. 4 (annotated); Pet. 47; Ex. 1003 ¶ 161).

Patent Owner also argues that one of the goals of Hernandez-Rosas's system is to allow use of different, ubiquitous display devices that users already have for other purposes, such as a mobile phone, tablet, smart watch, or desktop or laptop computer. *Id.* at 71 (citing Ex. 1007 ¶¶ 109, 122, 124, 127–128, Fig. 1). Patent Owner asserts that using NFC to exchange authentication information would have eliminated numerous display devices that Hernandez-Rosas teaches are desirable because “[t]ypical mobile phones, tablets, smart watches, and desktop and laptop computers were not NFC-enabled devices.” *Id.*

(iii) *Discussion*

Petitioner relies on testimony of its declarant, Dr. Kiaei, to support its contentions for a motivation to combine Hernandez-Rosas and Chivallier. Pet. 45–48 (citing Ex. 1003 ¶¶ 154–162). Specifically, Dr. Kiaei testifies that the range of NFC communication is ten centimeters or less. Ex. 1003 ¶ 157. Dr. Kiaei states that Hernandez-Rosas and Chivallier both disclose secure wireless communication with a display device and are thus in the same field as the '222 patent. *Id.* ¶ 158. In addition, Dr. Kiaei states that it would have been obvious to incorporate Chivallier's NFC in Hernandez-Rosas's CGM system so that the initial authentication and pairing process would be more secure. *Id.* ¶ 159. Furthermore, Dr. Kiaei states that using Chivallier's NFC in Hernandez Rosas's CGM system would “prevent the risk of eavesdropping that can occur with other longer-range wireless links.” *Id.* ¶ 160. Moreover, Dr. Kiaei states that the combination of Hernandez-Rosas and Chivallier combines 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 yielding 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). *Id.* ¶ 161. Dr. Kiaei also asserts that Petitioner’s proposed combination uses 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). *Id.* These rationales are recognized in *KSR* as supporting a motivation to combine. *See* 550 U.S. at 416–417.

Essentially, Patent Owner asserts that Chivallier’s NFC would not make Hernandez-Rosas’s CGM system any more secure since Hernandez-Rosas’s CGM system is already secured by its challenge, sensor identification, hash function, and the knowledge of how to use them to calculate a valid hash value. Patent Owner’s attorney argument contradicts Dr. Kiaei’s testimony that Chivallier’s NFC would make Hernandez-Rosas’s system more secure. Ex. 1003 ¶ 159; *see also Icon Health & Fitness, Inc. v. Strava, Inc.*, 849 F.3d 1034, 1043 (Fed. Cir. 2017) (“Attorney argument is not evidence”).

Weighing Patent Owner’s attorney argument against Dr. Kiaei’s testimony, we determine that Petitioner has shown sufficiently that a POSITA would have combined Chivallier’s NFC with Hernandez-Rosas’s CFM system for the reasons that Dr. Kiaei mentions. *Id.* ¶¶ 157–161.

Patent Owner may be correct that Petitioner’s reliance on Chivallier’s passive NFC tag would not have the capability to perform Hernandez-Rosas’s authentication. *See, e.g.*, Ex. 1003 ¶ 161. However, Petitioner also

stated that a POSITA would have been motivated to incorporate Chivallier's NFC *link* in Hernandez-Rosas's authentication. Pet. 47 (citing Ex. 1003 ¶¶ 158–161). Furthermore, Petitioner stated that NFC transmitters and receivers were well-known and it would have been within the skill of a POSITA to incorporate them in Hernandez-Rosas's CGM system with its existing wireless transceivers. *Id.* (citing Ex. 1003 ¶ 162). Accordingly, on the current record, Petitioner provides sufficient evidence of a motivation to combine Hernandez-Rosas and Chivallier notwithstanding Patent Owner's argument.

Patent Owner further argues that Hernandez-Rosas's mobile phones, tablets, smart watches, and desktop and laptop computers were not NFC-enabled. Prelim. Resp. 71. However, record evidence supports that NFC Forum was formed in 2004 to “*advanc[e]* the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs.” Ex. 1003 ¶ 33; Ex. 1012, 1. The word “advance” implies that NFC-enabled technologies had existed before NFC Forum was formed in 2004. Thus, Patent Owner's attorney argument is contradicted by Petitioner's evidence.

For the foregoing reasons, on this record, we determine that Petitioner shows sufficiently that a POSITA would have combined Hernandez-Rosas and Chivallier with a reasonable expectation of success.

4. *Claim 14*

Petitioner contends that claim 14 would have been obvious over the combination of Hernandez-Rosas and Chivallier. Pet. 48–70 (citing Ex. 1003 ¶¶ 163–198). Patent Owner does not dispute Petitioner's contentions that the combination of Hernandez-Rosas and Chivallier discloses each of the limitations of claim 14 at this time. We determine that

Petitioner demonstrates a reasonable likelihood to prevail in showing claim 14 would have been obvious over the combination of Hernandez-Rosas and Chivallier for the following reasons.

(i) *Preamble*

The preamble of claim 14 recites “A method for wireless communication of analyte data, the method comprising:” Ex. 1001, 116:58–59.

To the extent the preamble is limiting, Petitioner contends that Hernandez-Rosas discloses a method for wireless communication of analyte data. Pet. 48–49 (citing Ex. 1007, code (57), ¶¶ 7, 124–127, 140, Fig. 1).

Patent Owner does not dispute Petitioner’s contention that that Hernandez-Rosas discloses claim 14’s preamble.

On the present record, we find that Petitioner has shown sufficiently that the preamble of claim 14 is disclosed by Hernandez-Rosas, and thus do not reach the issue of whether the preamble is limiting.

(ii) *Limitation 14a: Measuring Analyte Values*

Limitation 14a recites “measuring analyte values in a host using a continuous analyte sensor of an analyte sensor system.” Ex. 1001, 116:60–61.

Petitioner contends that Hernandez-Rosas discloses a CGM system that measures analyte values using a “continuous analyte sensor.” Pet. 49–50 (citing Ex. 1007 ¶¶ 104, 124–125, 130, Fig. 3).

Patent Owner does not dispute Petitioner’s contention that that Hernandez-Rosas discloses limitation 14a.

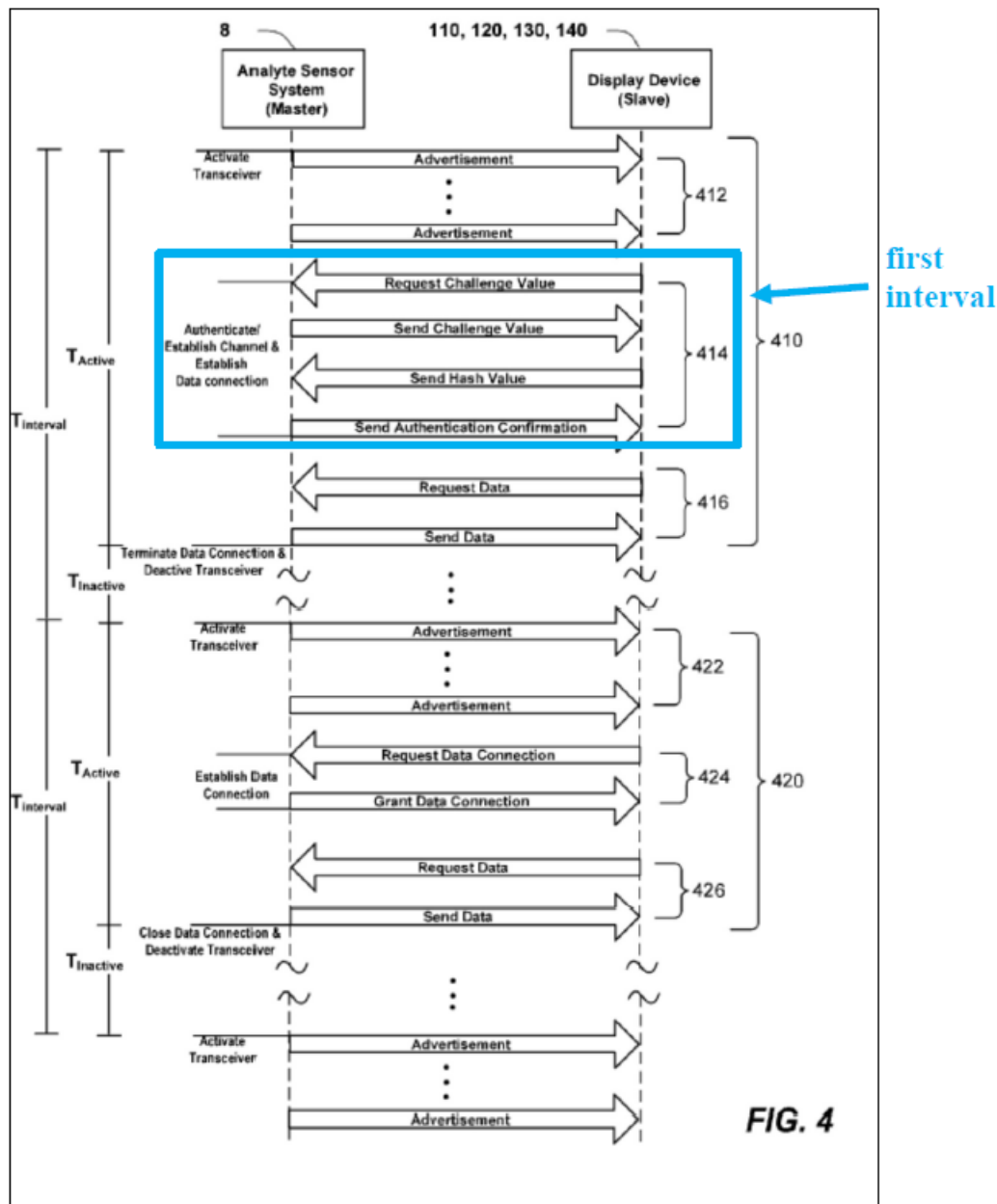
On the current record, we find that Petitioner shows sufficiently that Yarger discloses limitation 14a.

(iii) Limitation 14b: Using First Wireless Protocol

Limitation 14b recites “during a first interval, using a first wireless protocol to perform an exchange of information related to authentication with a display device.” Ex. 1001, 116:62–64.

Petitioner contends that 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. Pet. 51–55 (citing Ex. 1007, ¶¶ 16, 52, 119, 144, 147–150, 160 Figs. 3, 4, (annotated)).

Petitioner provides the following annotated version of Hernandez-Rosas’s Figure 4.



Petitioner annotates Hernandez-Rosas’s Figure 4 to show that the exchanges between the analyte sensor system 8 and display devices 110, 120, 130, 140 (Step 414 labeled “Authenticate/Establish Channel & Establish Data Connection”) occur during the first interval. The exchanges include “request challenge value”, “send challenge value”, “send hash value”, and “send authentication confirmation.”

Petitioner also contends that Chivallier discloses an authentication process that occurs in a first interval before a pairing process. *Id.* at 56–57 (citing Ex. 1008 ¶ 29, Fig. 4 (annotated)).

Patent Owner does not dispute Petitioner’s contentions that Hernandez-Rosas and Chivallier each disclose limitation 14b.

On the current record, we find that Petitioner shows sufficiently that the combination of Hernandez-Rosas and Chivallier discloses limitation 14b.

(iv) Limitation 14c: Determination for Triggering Alert

Limitation 14c recites “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.” Ex. 1001, 116:65–67.

Petitioner contends that “Hernandez-Rosas discloses that the system makes a determine 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.” Pet. 57 (citing Ex. 1007 ¶¶ 107–110, 112).

Patent Owner does not dispute Petitioner’s contention that Hernandez-Rosas discloses limitation 14c.

On the present record, we find that Petitioner shows sufficiently that limitation 14c is disclosed by Hernandez-Rosas.

(v) Limitation 14d: Triggering Alert and Providing Notification

Limitation 14d recites “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.” Ex. 1001, 117:1–4.

Petitioner contends that Hernandez-Rosas discloses limitation 14d. Pet. 57–58. Specifically, Petitioner contends that “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.” *Id.* at 58 (citing Ex. 1007 ¶¶ 107–109, 112).

Patent Owner does not dispute Petitioner’s contentions that Hernandez-Rosas disclose limitation 14d.

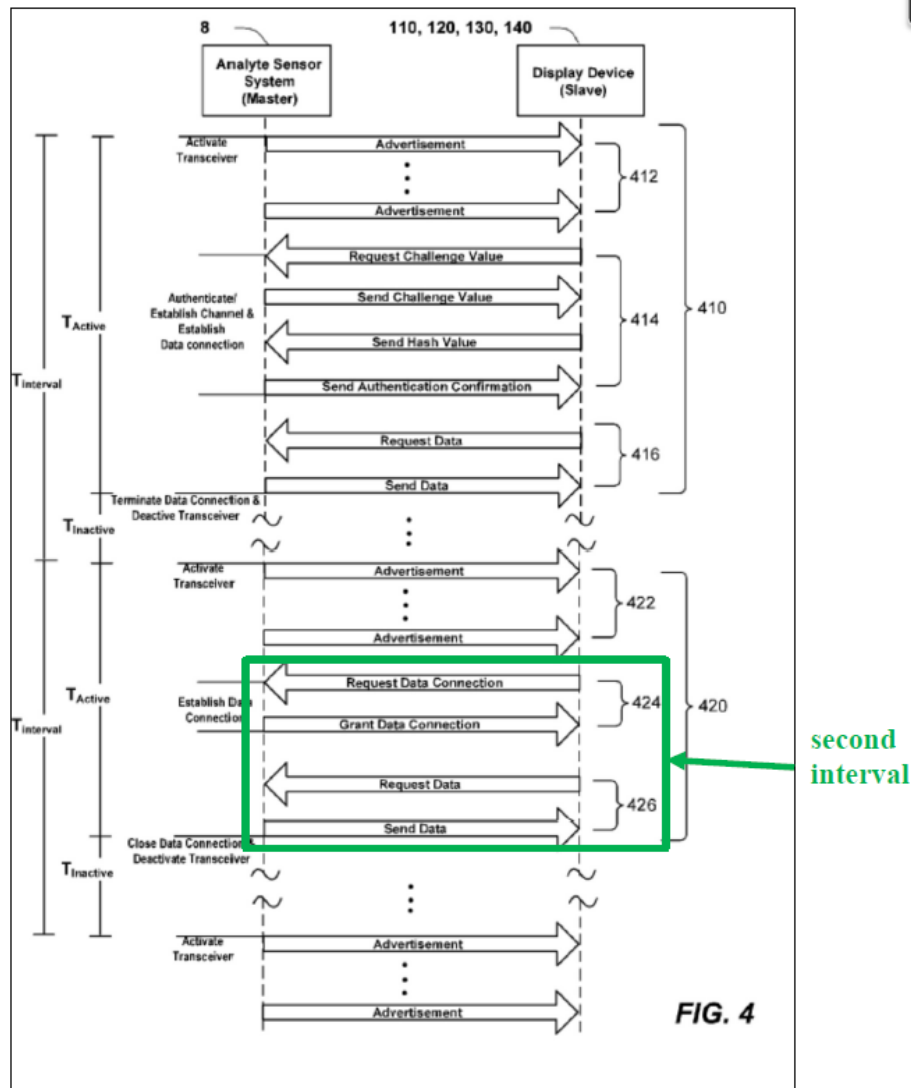
On this record, we find that Petitioner shows sufficiently that Hernandez-Rosas discloses limitation 14d.

(vi) *Limitation 14e: Using Second Wireless Protocol*

Limitation 14e recites “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.” Ex. 1001, 117:5–8.

Petitioner contends that “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.” Pet. 59–60 (citing Ex. 1007 ¶¶ 144, 147–152).

Petitioner provides an annotated version of Hernandez-Rosas’s Figure 4 shown below.



Id. at 60. Petitioner annotates Hernandez-Rosas’s Figure 4 in green to show information exchanges between the analyte sensor system 8 and display devices 110, 120, 130, 140 that Petitioner regards as bypassing authentication communications using a second protocol to transmit analyte data values from the analyte sensor system to the display devices during the second interval. *Id.* The information exchanges include “request data connection” and “grant data connection” in data connection process 424, and “request data” and “send data” in data communication process 426. *Id.*

Petitioner further contends that Hernandez-Rosas discloses that the data connection and communication processes bypass the authentication process. *Id.* at 59–61 (citing Ex. 1007 ¶ 152, Fig. 4 (annotated)).

In addition, Petitioner contends that Hernandez-Rosas discloses that the wireless data communication uses any of “WiFi, Bluetooth and Bluetooth low energy (BLE)” protocols” which differ from the NFC protocol used for authentication. *Id.* at 62–63 (citing Ex. 1007 ¶¶ 16, 52, 160).

Petitioner further asserts that Hernandez-Rosas and Chivallier each disclose that wireless data communication may be encrypted. *Id.* at 63–64 (citing Ex. 1007 ¶ 150; Ex. 1008 ¶ 31, Fig. 4 (annotated)).

Patent Owner does not dispute Petitioner’s contentions that Hernandez-Rosas and Chivallier disclose limitation 14e.

On the current record, we find that Petitioner demonstrates sufficiently that the combination of Hernandez-Rosas and Chivallier discloses limitation 14e.

(vii) Limitation 14f: Encrypted Analyte Value

Limitation 14f recites “wherein the encrypted analyte value has been generated using the information related to authentication.” Ex. 1001, 117:8–10.

Petitioner contends that Hernandez-Rosas discloses wireless data communication of analyte data values may be encrypted. Pet. 65 (citing Ex. 1007 ¶ 150). Petitioner states that Hernandez-Rosas does not explicitly state that analyte data values are encrypted using information related to authentication, but suggests that they are because decoding analyte values requires a key or code generated by identification information associated

with the analyte sensor system. *Id.* (citing Ex. 1007 ¶ 200, Figs. 4, 11; Ex. 1003 ¶ 188).

Petitioner further argues that Chivallier explicitly discloses that data concerning health parameters first encrypted during authentication using public and private keys are also used to encrypt data communications between a sensor and mobile device. *Id.* at 65–66 (citing Ex. 1008 ¶ 29).

Patent Owner does not dispute Petitioner’s contentions that Hernandez-Rosas and Chivallier disclose limitation 14f.

On the current record, we find that Petitioner demonstrates sufficiently that the combination of Hernandez-Rosas and Chivallier discloses limitation 14f.

(viii) Limitation 14g: Different Wireless Protocols

Limitation 14g recites “wherein the first wireless protocol is different than the second wireless protocol.” Ex. 1001, 117:10–11.

Petitioner contends that “Hernandez-Rosas discloses that the wireless data communication may utilize any number of protocols, including Wi-Fi, Bluetooth, and Bluetooth Low Energy protocols.” Pet. 66 (citing Ex. 1007 ¶ 160).

Petitioner asserts that “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.’” *Id.* at 67–68 (citing Ex. 1008 ¶¶ 16–17, Fig. 2).

Petitioner thus contends that, in the combination Hernandez-Rosas and Chivallier, “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).” *Id.* at 68.

Patent Owner does not dispute Petitioner’s contentions that Hernandez-Rosas and Chivallier disclose limitation 14g.

On the current record, we find that Petitioner demonstrates sufficiently that the combination of Hernandez-Rosas and Chivallier discloses limitation 14g.

(ix) *Limitation 14h: Neither Initiating Transmission Nor Providing Notification*

Limitation 14h recites “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.” Ex. 1001, 117:12–15.

Petitioner states that Hernandez-Rosas discloses that “Hernandez-Rosas discloses that authentication is ‘required’ prior to communicating data between the sensor and the display device.” Pet. 68–69 (citing Ex. 1007 ¶¶ 119, 149–150).

Petitioner asserts that

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.

Id. at 69 (citing Ex. 1003 ¶ 197).

Petitioner further contends that Chivallier transmits data only after it is authenticated. *Id.* at 69–70 (citing Ex. 1008 ¶ 34). Petitioner asserts that Chivallier discloses that its system can provide an alert if analysis of the transmitted data indicates a “critical result for the health of the patient.” *Id.* at 70 (citing Ex. 1008 ¶ 2). Petitioner argues that

Because Chivallier discloses that the alerts shown to the user are based on an analysis of the data transmitted by the sensor [citing Ex. 1008 ¶ 2], 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.

Id. at 70.

Patent Owner does not dispute Petitioner’s contentions that Hernandez-Rosas and Chivallier disclose limitation 14h.

On this record, we find that Petitioner shows sufficiently that the combination of Hernandez-Rosas and Chivallier discloses limitation 14h.

(x) *Conclusion for Claim 14*

Petitioner has shown sufficiently that a POSITA would have had reason to combine Hernandez-Rosas and Chivallier with a reasonable expectation of success, and that each limitation of claim 14 is disclosed by the combination.

Accordingly, on the current record, we determine that Petitioner has demonstrated a reasonable likelihood to prevail in demonstrating unpatentability of claim 14 of the ’222 patent as obvious over the combination of Hernandez-Rosas and Chivallier.

5. *Claim 15*

Claim 15 depends from claim 14 and recites “[15a] 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 [15b] wherein the second wireless protocol is selected from a group consisting of: WiFi communication, NFC and BLE communication.” Ex. 1001, 117:16–21.

Petitioner contends that the combination of Hernandez-Rosas and Chivallier renders claim 15 obvious. Pet. 70–73 (citing Ex. 1003 ¶¶ 199–205).

(i) *Limitation 15a: First Wireless Protocol*

Petitioner contends that “Hernandez-Rosas discloses that the wireless data communication may utilize any number of protocols, including Wi-Fi, Bluetooth, and Bluetooth Low Energy protocols.” Pet. 70.

Petitioner further asserts that “Chivallier explicitly teaches a CGM system where the ‘first wireless protocol’ used for the exchange of information related to authentication is NFC.” *Id.* at 71–72 (citing Ex. 1008 ¶ 17, Fig. 2).

Patent Owner does not dispute Petitioner’s contentions for limitation 15a.

On the present record, we find that Petitioner shows sufficiently that the combination of Hernandez-Rosas and Chivallier discloses limitation 15a.

(ii) *Limitation 15b: Second Wireless Protocol*

Petitioner contends that “Hernandez-Rosas discloses that the wireless data communication may utilize any number of protocols, including Wi-Fi, Bluetooth, and Bluetooth Low Energy.” Pet. 72.

Petitioner further contends that “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.’” *Id.* at 72–73 (citing Ex. 1008 ¶ 16, Fig. 2).

Patent Owner does not dispute Petitioner’s contentions for limitation 15b.

On the present record, we find that Petitioner shows sufficiently that Yarger discloses limitation 15b.

(iii) Conclusion for Claim 15

On this record, we determine that Petitioner presents a reasonable likelihood to prevail in demonstrating unpatentability of claim 15 as obvious over the combination of Hernandez-Rosas and Chivallier.

6. Claim 16

Claim 16 depends from claim 14 and recites “[16a] wherein the analyte sensor system is a continuous glucose sensor system and [16b] the information related to authentication comprises an application key.” Ex. 1001, 117:22–25.

Petitioner contends that the combination of Hernandez-Rosas and Chivallier renders claim 16 obvious. Pet. 73–75 (citing Ex. 1003 ¶¶ 206–210).

(i) Limitation 16a: Continuous Glucose System

Petitioner contends that Hernandez-Rosas discloses a CGM system for continuous measurement of an analyte (glucose) in a host. Pet. 73–74 (citing Ex. 1007 ¶¶ 104, 124–125, Fig. 1).

Patent Owner does not dispute Petitioner’s contention that Hernandez-Rosas discloses limitation 16a.

On the present record, we find that Petitioner shows sufficiently that Hernandez-Rosas discloses limitation 16a.

(ii) *Limitation 16b: Application Key*

Petitioner contends that “Hernandez-Rosas discloses that during the authentication process the sensor and control device exchange a ‘challenge value’ and ‘hash value based on the challenge value and the identification information associated with the analyte sensor.’” Pet. 74–75 (citing *id.* at § VI.A (limitation 14b)). Petitioner asserts that “the claimed ‘application key’ at least encompasses an exchange of challenge and hash values used to identify the sensor device or the display device.” *Id.* at 75.

Patent Owner does not dispute Petitioner’s contention that Hernandez-Rosas discloses limitation 16b.

On this record, Petitioner shows sufficiently that Hernandez-Rosas discloses limitation 16b.

(iii) *Conclusion for Claim 16*

On this record, Petitioner presents a reasonable likelihood to prevail in demonstrating unpatentability of claim 16 as obvious over the combination of Hernandez-Rosas and Chivallier.

7. *Claim 18*

Petitioner asserts that the combination of Hernandez-Rosas and Chivallier renders claim 18 obvious. Pet. 75–80 (citing Ex. 1003 ¶¶ 211–235). Patent Owner does not dispute Petitioner’s contentions that each limitation of claim 18 is disclosed by the combination of Hernandez-Rosas and Chivallier at this time. Below, we consider Petitioner’s contentions for each limitation of claim 18 and conclude that Petitioner has shown sufficiently that each limitation is disclosed by the combination.

(i) *Preamble*

The preamble of claim 18 recites “An analyte sensor system configured for wireless communication of analyte data, the analyte sensor system comprising.” Ex. 1001, 117:28–30.

Petitioner contends that “[t]o the extent the preamble is limiting, Hernandez-Rosas discloses a CGM system for wireless communication of analyte data” for the same reasons stated for claim 14’s preamble. Pet. 75.

Patent Owner does not dispute Petitioner’s contentions.

Because we find that Petitioner shows sufficiently on this record that the preamble of claim 18 is disclosed by Hernandez-Rosas, we do not decide whether the preamble is limiting.

(ii) *Limitation 18a: Sensor*

Limitation 18a recites “a continuous analyte sensor configured to measure analyte values in a host.” Ex. 1001, 117:31–32.

Petitioner contends that Hernandez-Rosas discloses limitation 18a for the same reasons stated for limitation 14a. Pet. 75.

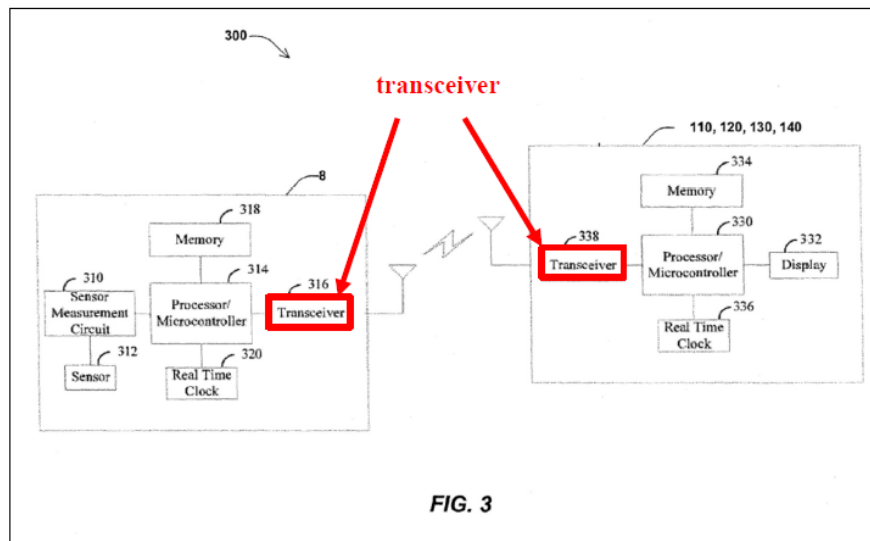
Patent Owner does not dispute Petitioner’s contentions.

On the present record, we find that Petitioner shows sufficiently that Hernandez-Rosas discloses limitation 18a.

(iii) *Limitation 18b: Transceiver*

Limitation 18b recites “a transceiver configured to transmit and receive wireless signals.” Ex. 1001, 117:33–34.

To explain its contentions for limitation 18b, Petitioner provides an annotated version of Hernandez-Rosas’s Figure 3 as shown below.



Petitioner annotates Hernandez-Rosas’s Figure 3 in red to show transceiver 316 in analyte sensor system 8 and transceiver 338 in display devices 110, 120, 130, 140. Pet. 76. Petitioner asserts that “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.” *Id.* at 75 (citing Ex. 1007 ¶¶ 139, 142, Fig. 3).

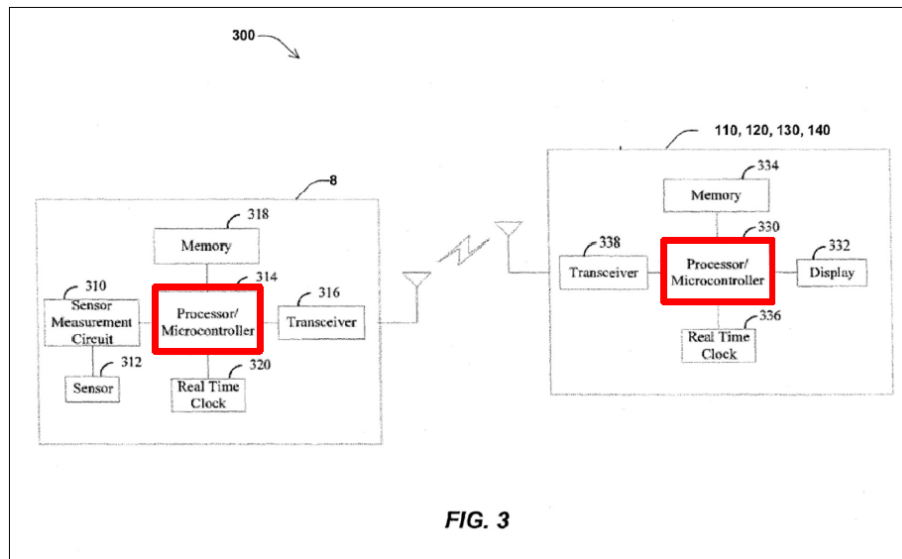
Patent Owner does not dispute Petitioner’s contentions.

On this record, we find that Petitioner shows sufficiently that Hernandez-Rosas discloses limitation 18b.

(iv) *Limitation 18c: Processor*

Limitation 18c recites “a processor operatively coupled to the analyte sensor and the transceiver and configured to cause the analyte sensor system to:” Ex. 1001, 117:35–37.

To explain its contentions for limitation 18c, Petitioner provides an annotated version of Hernandez-Rosas’s Figure 3 as shown below. Pet. 77.



Id. Petitioner annotates Hernandez-Rosas’s Figure 3 in red to show the processor/microcontroller 314 in the analyte sensor system 8, and the processor/microcontroller 330 in the display devices 110, 120, 130, 140. Petitioner contends that “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.” *Id.* at 76–77 (citing Ex. 1007 ¶¶ 139, 142).

Petitioner asserts that “[t]he 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.” *Id.* at 78 (citing Ex. 1007 ¶ 142). Petitioner asserts that “[s]imilarly, 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.* (citing Ex. 1007 ¶ 139). Petitioner

argues that “[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 limitations 18d–18j. *Id.* (citing Ex. 1003 ¶ 220).

Patent Owner does not dispute Petitioner’s contentions.

We find that Petitioner shows sufficiently that Hernandez-Rosas discloses limitation 18c.

(v) *Limitation 18d: Establishing First Connection*

Limitation 18d recites “during a first interval, establish a first connection between the analyte sensor system and a display device.” Ex. 1001, 117:38–40.

As explained for limitation 14b, Petitioner asserts that “Hernandez-Rosas discloses establishing a first connection during a first interval for exchanging information related to authentication between a sensor and a display device.” Pet. 78.

Patent Owner does not dispute Petitioner’s contentions.

We find that Petitioner shows sufficiently that limitation 18d is disclosed by Hernandez-Rosas.

(vi) *Limitation 18e: Exchange Information Related to Authentication*

Limitation 18e recites “during the first connection, exchange information related to authentication between the analyte sensor system and the display device.” Ex. 1001, 118:1–3.

Petitioner contends that, as explained for limitation 14b, “Hernandez-Rosas discloses exchanging information related to authentication with a display device during a first interval.” Pet. 79. We understand “during the

first connection” to be commensurate with “the first interval.” *See* Ex. 1007, Fig. 4 [Step 414].

Patent Owner does not dispute Petitioner’s contentions.

We find that Petitioner shows sufficiently that limitation 18e is disclosed by the combination of Hernandez-Rosas and Chivallier.

(vii) Limitation 18f: First Determination

Limitation 18f recites to “perform a first determination whether authentication was performed during the first interval.” Ex. 1001, 118:4–5.

Petitioner contends that, as explained for limitation 14h, “Hernandez-Rosas discloses that authentication is ‘required’ prior to communicating data between the sensor and the display device.” Pet. 79. Petitioner asserts that 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.” *Id.* (citing Ex. 1007 ¶ 150, Fig. 4). Petitioner avers that “[t]he verification of the authentication information corresponds to the claimed ‘first determination whether authentication was performed during the first interval.’” *Id.* at 79–80.

In addition, Petitioner contends that, as explained for limitation 14h, “Chivallier also discloses that data is ‘only transmitted after authentication’ in order to provide a high-level of security for the user data.” *Id.* at 80. Petitioner asserts that “[t]he 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.’” *Id.*

Patent Owner does not dispute Petitioner’s contentions.

On this record, we find that Petitioner shows sufficiently that limitation 18f is disclosed by the combination of Hernandez-Rosas and Chivallier.

(viii) Limitation 18g: Second Determination

Limitation 18g recites “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.” Ex. 1001, 118:6–8.

Petitioner asserts that limitation 18g is disclosed by the combination of Hernandez-Rosas and Chivallier for the reasons stated for limitation 14c.

Patent Owner does not dispute Petitioner’s contentions for limitation 18g.

On this record, we find that Petitioner shows sufficiently that limitation 18g is disclosed by Hernandez-Rosas.

(ix) Limitation 18h: Trigger Alert and Provide Notification

Limitation 18h recites “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.” Ex. 1001, 118:9–12.

Petitioner asserts that limitation 18h is disclosed by Hernandez-Rosas for the reasons stated for limitation 14d.

Patent Owner does not dispute Petitioner’s contentions.

On this record, we find that Petitioner shows sufficiently that limitation 18h is disclosed Hernandez-Rosas for the reasons stated for limitation 14d.

(x) Limitation 18i: Transmit Encrypted Analyte Value

Limitation 18i recites “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.” Ex. 1001, 118:13–16.

Petitioner asserts that limitation 18i is disclosed by the combination of Hernandez-Rosas and Chivallier for the reasons stated for limitation 14e.

Patent Owner does not dispute Petitioner’s contentions.

On this record, we find that Petitioner shows sufficiently that limitation 18i is disclosed by the combination of Hernandez-Rosas and Chivallier based on the evidence Petitioner provided for limitation 14e.

(xi) Limitation 18j: Neither Initiate Transmission Nor Provide Notification

Limitation 18j recites “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.” Ex. 1001, 118:16–21.

Petitioner asserts that limitation 18j is disclosed by the combination of Hernandez-Rosas and Chivallier for the reasons stated for limitation 14h.

Patent Owner does not dispute Petitioner’s contentions.

On the current record, we find that Petitioner shows sufficiently that limitation 18j is disclosed by the combination of Hernandez-Rosas and Chivallier on the evidence Petitioner provided for limitation 14h.

(xii) Conclusion for Claim 18

Petitioner shows sufficiently on the present record that a POSITA would have been motivated to combine Hernandez-Rosas and Chivallier with a reasonable expectation of success notwithstanding Patent Owner’s

arguments. *See* § III.D.3, *supra*. Petitioner further shows that each limitation of claim 18 is disclosed by the combination of Hernandez-Rosas and Chivallier, and Patent Owner does not dispute these contentions at this time. Accordingly, Petitioner presents a reasonable likelihood to prevail in demonstrating unpatentability of claim 18 as obvious over the combination of Hernandez-Rosas and Chivallier.

8. *Claim 19*

Claim 19 depends from claim 18 and recites “[19a] 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 [19b] during the second connection, bypass the exchange of the information related to authentication.” Ex. 1001, 118:22–29.

(i) *Limitation 19a: Second Connection*

Petitioner asserts that limitation 19a is disclosed by the combination of Hernandez-Rosas and Chivallier for the reasons stated for limitation 14h.

Patent Owner does not dispute Petitioner’s contentions.

On this record, we find that Petitioner shows sufficiently that limitation 19a is disclosed by the combination of Hernandez-Rosas and Chivallier based on the evidence that Petitioner provided for limitation 14e.

(ii) *Limitation 19b: Bypass Exchange of Information Related to Authentication*

Petitioner asserts that limitation 19b is disclosed by the combination of Hernandez-Rosas and Chivallier for the reasons stated for limitation 14e.

Patent Owner does not dispute Petitioner’s contentions.

On this record, Petitioner shows sufficiently that limitation 19b is disclosed by the combination of Hernandez-Rosas and Chivallier based on the evidence that Petitioner provided for limitation 14e.

(iii) *Conclusion for Claim 19*

On the current record, Petitioner presents a reasonable likelihood to prevail in demonstrating unpatentability of claim 19 as obvious over the combination of Hernandez-Rosas and Chivallier.

9. *Claim 20*

Claim 20 depends from claim 19 and recites

[20a] wherein the analyte sensor system is a continuous glucose sensor system, and [20b] the information related to authentication comprises an application key [20c] 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 [20d] wherein the use of the application key allows the analyte sensor system to bypass the exchange.

Ex. 1001, 118:30–39.

Petitioner contends that the combination of Hernandez-Rosas and Chivallier renders claim 20 obvious for the reasons discussed for each limitation below. Pet. 81 (citing Ex. 1003 ¶¶ 241–248).

(i) *Limitation 20a: Continuous Glucose Sensor System*

Petitioner contends that Hernandez-Rosas discloses limitation 20a for the reasons stated in the Petition for limitation 16a. Pet. 82.

Patent Owner does not dispute Petitioner’s contention that Hernandez-Rosas discloses limitation 20a.

On this record, Petitioner shows sufficiently that Hernandez-Rosas discloses limitation 20a.

(ii) *Limitation 20b: Application Key*

Petitioner contends that Hernandez-Rosas discloses limitation 20b for the reasons stated in the Petition for limitation 16b. Pet. 82.

Patent Owner does not dispute Petitioner's contention that Hernandez-Rosas discloses limitation 20b.

On this record, Petitioner shows sufficiently that Hernandez-Rosas discloses limitation 20b.

(iii) *Limitation 20c: Processor*

Petitioner contends that, as explained in the Petition for limitations 14b and 16b, "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 . . . this hash value of the challenge value and identification information corresponds to the 'application key.'" Pet. 82. Petitioner asserts that, as explained in the Petition for limitation 14f, "Hernandez-Rosas discloses that this information relating to identification can be used to encrypt the analyte data in a CGM system." *Id.* Accordingly, Petitioner states that "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." *Id.*

Patent Owner does not dispute Petitioner's contentions that Hernandez-Rosas discloses limitation 20c.

On this record, Petitioner shows sufficiently that Hernandez-Rosas discloses limitation 20c.

(iv) *Limitation 20d: Application Key Allows Bypass*

Petitioner contends that Hernandez-Rosas discloses limitation 20d for the reasons stated in the Petition for limitation 14e. Pet. 83.

Patent Owner does not dispute Petitioner's contentions that Hernandez-Rosas discloses limitation 20d.

On this record, Petitioner shows sufficiently that Hernandez-Rosas discloses limitation 20d.

(v) *Conclusion for Claim 20*

On the current record, Petitioner presents a reasonable likelihood to prevail in demonstrating unpatentability of claim 20 as obvious over the combination of Hernandez-Rosas and Chivallier.

IV. CONCLUSION

For the above reasons, we conclude the record demonstrates a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, so we grant institution of the petitioned *inter partes* review per 35 U.S.C. § 314(a) for all challenged claims and all grounds. *See* 37 C.F.R. § 42.108(a).

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), the petitioned institution of *inter partes* review of claims 14–16 and 18–20 of the '222 patent is *granted*; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial and that the trial will commence on the entry date of this decision.

IPR2024-00797
Patent 10,375,222 B2

FOR PETITIONER:

Scott C. Weidenfeller
Peter P. Chen
David. A. Garr
COVINGTON & BURLING LLP
sweidenfeller@cov.com
pchen@cov.com
dgarr@cov.com

FOR PATENT OWNER:

Elisabeth H. Hunt
Richard F. Giunta
Marc S. Johannes
WOLF GREENFIELD & SACKS, P.C.
EHunt-PTAB@wolfgreenfield.com
RGiunta-PTAB@wolfgreenfield.com
MJohannes-PTAB@wolfgreenfield.com