

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DATAVANT, INC.,
Petitioner,

v.

VIGILYTICS LLC,
Patent Owner.

IPR2024-00381
Patent 10,886,012 B1

Before THOMAS L. GIANNETTI, BRIAN J. McNAMARA, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

AMUNDSON, *Administrative Patent Judge*.

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

I. INTRODUCTION

Datavant, Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–20 in U.S. Patent No. 10,886,012 B1 (Exhibit 1001, “the ’012 patent”) under 35 U.S.C. §§ 311–319. Paper 2 (“Pet.”). Vigilytics LLC (“Patent Owner”) did not file a Preliminary Response.

Under 37 C.F.R. § 42.4(a), we have authority to determine whether to institute an *inter partes* review. We may institute an *inter partes* review only if “the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a) (2018). The “reasonable likelihood” standard is “a higher standard than mere notice pleading” but “lower than the ‘preponderance’ standard to prevail in a final written decision.” *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential).

Based on the current record and for the reasons explained below, Petitioner has shown that there is a reasonable likelihood that it would prevail with respect to at least one of the challenged claims. Thus, we institute an *inter partes* review of claims 1–20 in the ’012 patent on all challenges included in the Petition.

II. BACKGROUND

A. *Real Parties in Interest*

Petitioner identifies the following real parties in interest: Datavant, Inc. and Ciox Health LLC. Pet. 1. Patent Owner identifies itself as the sole real party in interest. Paper 3, 1. The parties do not raise any issue about real parties in interest.

B. Related Matters

Petitioner and Patent Owner identify the following civil action as a related matter involving the '012 patent: *Milliman, Inc. et al. v. Gradient A.I. Corp. et. al.*, No. 1:21-cv-10865 (D. Mass. filed May 25, 2021) (the “Massachusetts case”). Pet. 1; Paper 3, 1.

C. The '012 Patent (Exhibit 1001)

The '012 patent, titled “De-Identifying Medical History Information for Medical Underwriting,” issued on January 5, 2021, from an application filed on September 14, 2018. Ex. 1001, codes (22), (45), (54). The '012 patent identifies that application as the latest in a series of continuation applications with the initial application filed on June 30, 2010. *Id.* at 1:7–11, code (63). The '012 patent notes that the initial application “claims benefit” to a provisional application filed on July 1, 2009. *Id.* at 1:10–12.

The '012 patent explains that federal privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA), generally prohibit the disclosure of protected health information (PHI) without an individual’s authorization. Ex. 1001, 1:37–40, 4:5–8, 4:24–26. As an example of an issue resulting from federal privacy laws, the patent explains that insurance companies that “offer health insurance to small and midsize groups (containing 10–1000 individuals) are often unable to obtain the health history data they need to estimate the risk of insuring such groups.” *Id.* at 1:21–25; *see id.* at 4:11–26.

To address that issue and other issues, the '012 patent discloses systems and methods that “relate to de-identifying medical history information.” Ex. 1001, 1:44–45. For example, “a computer-implemented method includes producing information that characterizes a group of

individuals from a set of private data representing characteristics of the individuals.” *Id.* at 1:46–49. “The identity of the individuals is unattainable from the produced information.” *Id.* at 1:49–50. “The method also includes providing the produced information to report the characteristics of the group.” *Id.* at 1:50–52.

Producing information that “characterizes the group” may include the following steps:

- (1) “determining if the group includes at least a minimum number of individuals”;
- (2) “producing a request token for each individual included in the group,” e.g., by “encrypting respective data that identifies each individual”;
- (3) “comparing the request tokens to tokens associated with the information to be produced” where the “tokens associated with the information to be produced and the request tokens may be similarly encrypted”;
- (4) “determining if the comparison provides at least a minimum number of matches”; and
- (5) “requesting a predefined portion of the information.”

Ex. 1001, 1:54–2:3.

A system according to the ’012 patent may include “an encryption server for producing a request token of each individual included in a group identified in a request for information that characterizes the group.”

Ex. 1001, 2:5–8. The encryption server “may be configured to determine if the group includes at least a minimum number of individuals.” *Id.* at 2:29–32.

A system according to the ’012 patent may include “a data server for producing the information that characterizes the group from a set of private

data representing characteristics of the individuals.” Ex. 1001, 2:8–11. The data server “may be configured to compare the request tokens to tokens associated with the information to be produced” where the “tokens associated with the information to be produced and the request tokens may be similarly encrypted.” *Id.* at 2:21–25. The data server “may be configured to determine if the comparison provides at least a minimum number of matches.” *Id.* at 2:25–27.

The ’012 patent’s Figure 3 (reproduced below) depicts a system for producing information that characterizes a group of individuals from a set of private data representing characteristics of the individuals:

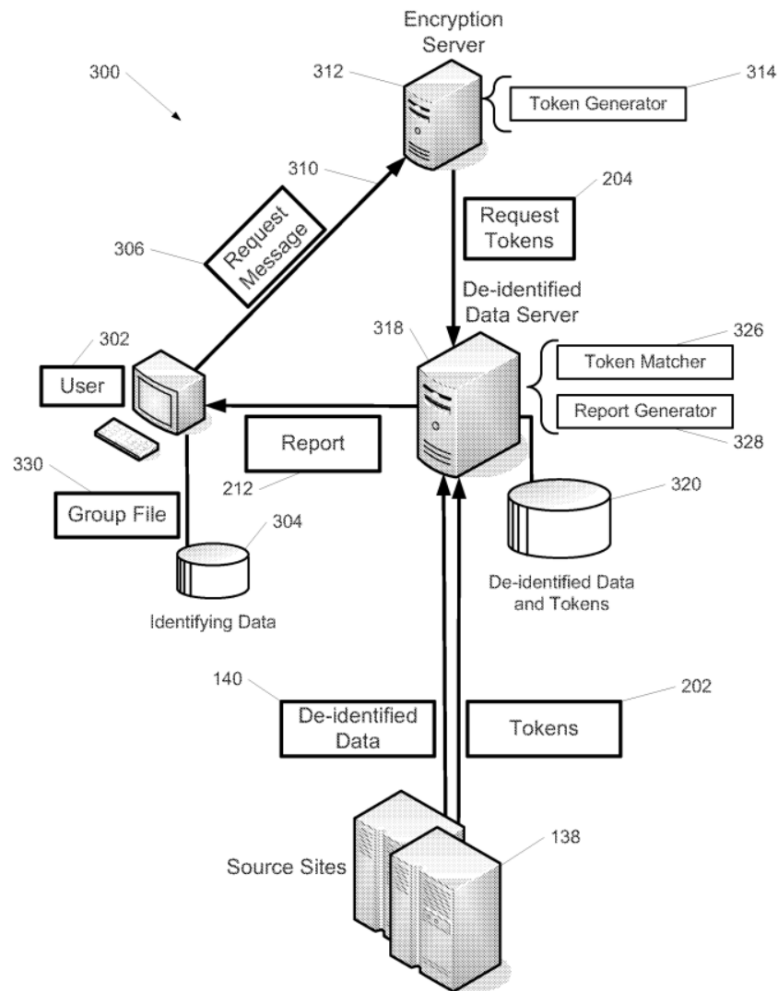


FIG. 3

Figure 3 illustrates “exemplary system 300” including user 302 who has a computing device, encryption server 312, de-identified data server 318, and “source sites 138 for de-identified data,” such as “pharmacies, healthcare professionals and electronic claims clearing houses.” Ex. 1001, 3:58–60, 5:14–16, 5:52–57, Fig. 3.

User 302 specifies “a group of people using identifying data for each group member” and generates request message 306, e.g., “a computer file,” that “uniquely identifies each member of the group using the identifying

data 304.” Ex. 1001, 5:14–16, 5:20–25. “Typically, the group contains at least a minimum number of unique members.” *Id.* at 5:23–24.

If “the request message 306 contains a minimum number of group members,” encryption server 312 “creates a unique token, or identifier, for each person in the message 306” by “applying a token generator 314 that encrypts the personally identifiable information [PII] of each group member.” Ex. 1001, 5:41–46. “The set of tokens corresponding to all the group members constitutes a batch of request tokens 204.” *Id.* at 5:46–48.

Encryption server 312 “provides the request tokens 204” to de-identified data server 318. Ex. 1001, 5:52–53. De-identified data server 318 “stores records of de-identified data and corresponding tokens 320 obtained from source sites 138.” *Id.* at 5:53–55. “Each token obtained from the source sites 138 may have been created using the same token generator 314” used by encryption server 312 or “using any other means that generates the identical token for the same personally identifiable information.” *Id.* at 5:57–61.

De-identified data server 318 executes token matcher 326 that “performs a look-up in the de-identified database 320 to find all tokens in the database that match the tokens” sent by encryption server 312. Ex. 1001, 6:10–14. “All available data for matched tokens, the requested de-identified data 208, is retrieved for use in the report generator 328.” *Id.* at 6:14–16. “The report generator formats the processed data into an electronic or hardcopy report 212 that is returned to the user.” *Id.* at 6:23–25.

D. The Challenged Claims

The '012 patent includes 20 claims as follows:

- (i) independent claim 1 for “[a] user computing device-implemented method”;
- (ii) claims 2–6 that depend directly from claim 1;
- (iii) independent claim 7 for “[a] system”;
- (iv) claims 8–13 that depend directly from claim 7;
- (v) independent claim 14 for “[o]ne or more computer readable storage devices storing instructions”; and
- (vi) claims 15–20 that depend directly from claim 14.

Ex. 1001, 10:42–12:48. Petitioner challenges all 20 claims in the '012 patent. Pet. 9–75.

Claims 1 and 7 exemplify the challenged claims and read as follows (with formatting added for clarity and with bracketed numbers and letters added for reference purposes):¹

1. [1.a] A user computing device-implemented method comprising:

[1.a] producing, by a processor of the user computing device, an encrypted request message for healthcare information that characterizes a group composed of multiple individuals,

[1.b] the encrypted request message including a unique token produced by the user device for each individual included in the group;

[1.c] sending the encrypted request message to a server to produce the healthcare information,

¹ We use the same numbers and letters that Petitioner uses to identify the claim language. See Pet. iv–v (Claim Listing).

[1.d] the server is configured to compare the unique request tokens to unique tokens associated with healthcare data to find matching tokens,

[1.e] the unique tokens associated with healthcare data are absent identities of individuals,

[1.f] the healthcare information being produced based on a minimum number of matched tokens and the identity of the individuals being unattainable from the produced healthcare information; and

[1.g] receiving, at the user computing device, the produced healthcare information to report the characteristics of the group [1.h] absent authorization from the individuals in the group.

7. [7.a] A system comprising:

[7.a] a user computing device [7.b] that produces an encrypted request message for healthcare information that characterizes a group composed of multiple individuals,

[7.c] the encrypted request message including a unique token produced by the user device for each individual included in the group,

[7.d] wherein the user computing device is configured to send the encrypted request message to a server to produce the healthcare information,

[7.e] the server is configured to compare the unique request tokens to unique tokens associated with healthcare data to find matching tokens,

[7.f] the unique tokens associated with healthcare data are absent identities of individuals,

[7.g] the healthcare information being produced based on a minimum number of matched tokens and

[7.h] the identity of the individuals being unattainable from the produced healthcare information,

[7.i] wherein the user computing device is further configured to receive the produced healthcare information to

report the characteristics of the group [7.j] absent authorization from the individuals in the group.

Ex. 1001, 10:42–63, 11:16–36.

E. The Asserted References

For its challenge, Petitioner relies on the following references:

Name	Reference	Exhibit
Evenhaim	US 7,823,207 B2, issued October 26, 2010 (based on an application filed April 1, 2005)	1005
Settimi	US 2007/0294111 A1, published December 20, 2007 (based on an application filed November 20, 2006)	1006
Dick	US 2002/0111833 A1, published August 15, 2002 (based on an application filed January 23, 2002)	1007
Landi	US 7,519,591 B2, issued April 14, 2009 (based on an application filed March 9, 2004)	1008
Murphy	Shawn N. Murphy & Henry C. Chueh, <i>A Security Architecture for Query Tools Used to Access Large Biomedical Databases</i> , in <i>Bio*medical Informatics: One Discipline: The Annual Symposium of the American Medical Informatics Association Proceedings</i> , 552–56 (Isaac S. Kohane ed., 2002)	1009

Pet. 9–75. Petitioner asserts that each reference qualifies as prior art “under at least 35 U.S.C. § 102(b) (pre-AIA).” *Id.* at 9, 14, 37, 54–55; *see* 35 U.S.C. § 102(b) (2006).²

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. § 102 and § 103 effective March 16, 2013. Because the effective filing date of the challenged claims predates the AIA’s amendments to § 102 and § 103, this decision refers to the pre-AIA versions of § 102 and § 103.

F. The Asserted Challenge to Patentability

Petitioner asserts the following challenges to patentability:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–20	103(a)	Evenhaim, Murphy
1–20	103(a)	Evenhaim, Settimi, Murphy
1–20	103(a)	Dick, Landi, Murphy

Pet. 9–75.

G. Testimonial Evidence

To support its challenge, Petitioner relies on the declaration of Paul C. Clark, DSc. (Exhibit 1003). Dr. Clark states that he received various degrees as follows:

- (1) “a Bachelor of Science degree in Mathematics from the University of California, Irvine” in 1986;
- (2) “a Master of Science degree in Electrical Engineering and Computer Science from the University of Southern California” in 1988; and
- (3) “a Doctor of Science degree in Computer Science from George Washington University” in 1994.

Ex. 1003 ¶ 4. Dr. Clark also states, “I have been retained by Venable LLP, counsel for [Petitioner] to provide my opinions concerning the validity of” claims 1–20 in the ’012 patent. *Id.* ¶ 1.

Further, Petitioner relies on the declaration of Sylvia D. Hall-Ellis, Ph.D. (Exhibit 1013) to establish the authenticity and public accessibility of Murphy.

III. PATENTABILITY ANALYSIS

A. Legal Principles: Obviousness

A patent may not be obtained “if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” 35 U.S.C. § 103(a) (2006). An obviousness analysis involves underlying factual inquiries including (1) the scope and content of the prior art; (2) differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) where in evidence, objective indicia of nonobviousness, such as commercial success, long-felt but unsolved needs, and failure of others.³ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18, 35–36 (1966); *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1047–48 (Fed. Cir. 2016) (en banc). When evaluating a combination of references, an obviousness analysis should address “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

We analyze the obviousness issues according to these principles.

B. Level of Ordinary Skill in the Art

Factors pertinent to determining the level of ordinary skill in the art include (1) the educational level of the inventor; (2) the type of problems encountered in the art; (3) prior-art solutions to those problems; (4) the rapidity with which innovations are made; (5) the sophistication of the technology; and (6) the educational level of workers active in the field.

³ Petitioner and Dr. Clark do not address any objective indicia of nonobviousness. *See, e.g.*, Pet. 6–7, 9–75; Ex. 1003 ¶¶ 30–36, 67–269.

Envtl. Designs, Ltd. v. Union Oil Co., 713 F.2d 693, 696–97 (Fed. Cir. 1983). Not all factors may exist in every case, and one or more of these or other factors may predominate in a particular case. *Id.* These factors are not exhaustive, but merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007). Moreover, the prior art itself may reflect an appropriate skill level. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Petitioner asserts that a person of ordinary skill in the art at the time of the alleged invention would have had “a Bachelor of Science degree in computer science, or a related field, and at least two years of experience in the field of computer science, focusing on data privacy, computer networking, and/or data records management.” Pet. 8. Petitioner also asserts that “[s]uperior education could compensate for less work experience, and vice-versa.” *Id.* Dr. Clark’s testimony supports Petitioner’s assertions. *See* Ex. 1003 ¶ 23.

Based on the current record and for purposes of this decision, we accept Petitioner’s description of an ordinarily skilled artisan because it comports with the technology and claims of the ’012 patent as well as the asserted references.

C. Claim Construction

We construe claim terms “using the same claim construction standard” that district courts use to construe claim terms in civil actions under 35 U.S.C. § 282(b). *See* 37 C.F.R. § 42.100(b) (2023). Under that standard, claim terms “are given their ordinary and customary meaning, which is the meaning the term would have to a person of ordinary skill in the art at the time of the invention.” *Power Integrations, Inc. v. Fairchild*

Semiconductor Int'l, Inc., 904 F.3d 965, 971 (Fed. Cir. 2018) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc)). The meaning of claim terms may be determined by “look[ing] principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

For this proceeding, Petitioner “adopts” the following constructions that Patent Owner proposed in the Massachusetts case:

- (1) “token” means “[a]n identifier associated with an individual that does not reveal the identity of the individual”;
- (2) “server” means “[a] computer, with a processor and memory, on a network that provides information in response to requests from another computer”; and
- (3) “similarly encrypted” means “[g]enerated such that tokens generated from corresponding information can be compared to one another to detect a match.”

Pet. 7–8; *see* Ex. 1010, 9, 11, 14.⁴ Petitioner does not propose an explicit construction for any other claim term. *See, e.g.*, Pet. 7–75. As Petitioner expressly “adopts” the above constructions, we understand Petitioner’s adoption to satisfy the Board’s requirement that a petition specify “[h]ow the challenged claim is to be construed.” *See* 37 C.F.R. § 42.104(b)(3).

“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.” *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); *see Nidec Motor*

⁴ For Exhibit 1010 (Plaintiffs’ Opening Claim Construction Brief), we cite to the page numbers of the brief rather than the header page numbers.

Corp. v. Zhongshan Broad Ocean Motor Co., 868 F.3d 1013, 1017 (Fed. Cir. 2017). Based on the current record, we determine that no claim term requires an explicit construction to decide whether Petitioner satisfies the “reasonable likelihood” standard for instituting trial.

*D. Alleged Obviousness over
Evenhaim and Murphy: Claims 1–20*

Petitioner contends that claims 1–20 are unpatentable under § 103(a) as obvious over Evenhaim and Murphy. *See* Pet. 9–37. Below, we provide overviews of Evenhaim and Murphy. Then, we consider obviousness issues. As explained below, Petitioner establishes sufficiently for purposes of institution that the combined disclosures in Evenhaim and Murphy teach the subject matter in claims 1–20.

1. OVERVIEW OF EVENHAIM (EXHIBIT 1005)

Evenhaim is a U.S. patent titled “Privacy Preserving Data-Mining Protocol,” filed on April 1, 2005, and issued on October 26, 2010. Ex. 1005, codes (12), (22), (45), (54). Evenhaim states that the invention “relates to coordination of data privileges while simultaneously preserving data privacy and allowing useful facilitation of privacy sensitive data features.” *Id.* at 1:16–19; *see id.* at code (57).

Evenhaim explains that “healthcare organizations such as physician practices, labs, hospitals and health maintenance organizations (HMOs) keep extensive medical records including data on each specific patient and on each specific doctor.” Ex. 1005, 1:54–58. But HIPAA “prevents HMOs and healthcare providers from sharing data at full transparency” since “the privacy of individuals must be preserved.” *Id.* at 1:58–62. If pharmaceutical companies had “unrestricted access to the HMO raw data,” however, they

“could greatly improve many technical and mercantile aspects of their operation.” *Id.* at 1:63–67.

According to Evenhaim, “there is a long felt need in the art for a protocol that will allow higher resolution query and manipulation of privacy sensitive data while simultaneously allowing individual privacy to be preserved.” Ex. 1005, 5:4–7. Evenhaim endeavors to address that need by providing a “Privacy Preserving Data-Mining Protocol.” *Id.* at 6:49–52.

Evenhaim’s protocol operates between a secure “aggregator” data processor and one or more secure “source-entity” data processors with the various processors “interconnected via an electronic data-communications topology,” such as the Internet. Ex. 1005, 6:57–62, 7:53–56, 7:59–61, 12:51–53. The aggregator processor “is a central data processing machine.” *Id.* at 7:33–34. The one or more source-entity processors “are other data processing machines that respectively include records having privacy identified data such as name, identity number, or the likes.” *Id.* at 7:34–38; *see id.* at 7:61–63.

In Evenhaim’s protocol, the following steps occur at an aggregator processor:

- (i) accepting from a user interface “a query against a plurality of the predetermined attributes and therewith forming a parameter list”;
- (ii) transmitting “the parameter list to each of the ‘source-entity’ processors”;
- (iii) receiving “a respective file from each of the ‘source-entity’ processors”;
- (iv) aggregating “the plurality of files into a data-warehouse”;
- (v) extracting “query relevant data from the data-warehouse” using the parameter list;

- (vi) agglomerating the extract; and
- (vii) reporting the agglomerated extract to a user interface.

Ex. 1005, 6:64–7:11, Fig. 3; *see id.* at 7:64–9:28, 10:29–36, 10:55–11:13, 11:40–43, Figs. 6, 8.

In Evenhaim’s protocol, the following steps occur at a source-entity processor:

- (i) accumulating “data-items wherein some of the data-items have privacy sensitive micro-data”;
- (ii) organizing “the data-items using the plurality of predetermined attributes”;
- (iii) receiving “a parameter list from the ‘aggregator’ processor”;
- (iv) forming “a file by ‘crunching together’ the data-items according to the parameter list”;
- (v) filtering out “portions of the file which characterize details particular to less than a predetermined quantity of micro-data-specific data-items”; and
- (vi) transmitting “the file to the ‘aggregator’ processor.”

Ex. 1005, 7:12–26, Fig. 3; *see id.* at 9:29–67, 10:18–28, 10:37–41, 10:46–54, 11:14–29, 11:34–40, Figs. 7–8.

The parameter list may include “identity-disclosing specifics,” such as “name, personal identity number or simple data combinations that would allow breach of privacy.” Ex. 1005, 8:10–13; *see id.* at 8:1–4, 8:41–43. Importantly, however, “these identity-disclosing specifics are part of a large enough list in the processing of a query so that the query result will present sufficient statistical distribution to protect the ‘reverse engineering’ of the result back to any individual in the initial query list.” *Id.* at 8:13–18; *see id.*

at 8:43–47, 13:62–66, 16:26–30. Additionally, “all or part of the parameter list is encrypted.” *Id.* at 8:47–48; *see id.* at 14:6–7.

Evenhaim discloses “interim data merger enabled embodiments” that employ “imbedded encryption strategies for micro-data” and “allow for the linkage of data items as related to a common entity.” Ex. 1005, 12:4–8, 13:21–26. “If the data sources are careful to encrypt the identifying portions of each record using a common encryption ‘key’, then further down the data processing circuit it will be possible to link records related to a common individual without compromising the identity of that individual.” *Id.* at 12:12–16. For instance, an individual’s identity information “is replaced with a unique encryption key, such as a one way hash or Advanced Encryption Standard (AES) or the likes.” *Id.* at 12:39–42; *see id.* at 12:61–63. Thus, “the ability to link micro-level records related to the same identity at the data aggregator level is preserved—even if the records came from two different data sources.” *Id.* at 12:48–52; *see id.* at 12:42–47.

Further, “every step requiring a transmitting of data (or of at least one file) and every respective associated step requiring receiving of that data (or of that at least one file) may preferably include respective encryption and decryption.” Ex. 1005, 13:33–36; *see id.* at 15:61–65.

Evenhaim's Figure 4 (reproduced below) depicts a preferred embodiment of Evenhaim's protocol:

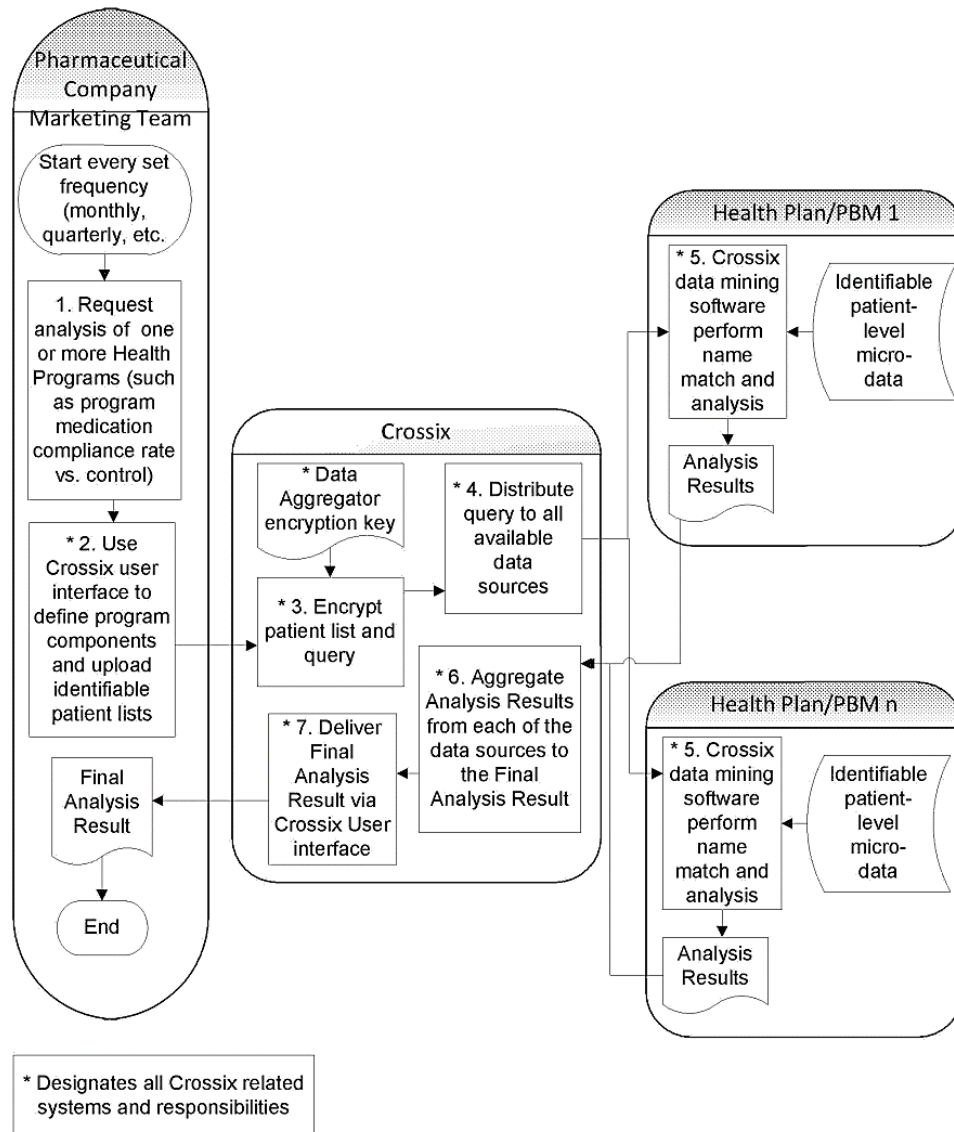


FIG. 4

Figure 4 illustrates “detailed aspects” of Evenhaim’s protocol for an example from the healthcare industry where a pharmaceutical company’s marketing team seeks information from multiple Health Plans (HPs) or Pharmacy Benefit Managers (PBMs). Ex. 1005, 14:48–49, 14:56–59, 15:25–16:35, Fig. 4.

In boxes 1 and 2 in Figure 4, the marketing team provides a query seeking statistics from the HPs/PBMs concerning a group of persons that are identified by name (or the like) in a parameter list. Ex. 1005, 7:65–8:43, 9:6–10, Fig. 4.

In boxes 3 and 4 in Figure 4, an aggregator processor uses an encryption key to encrypt the protected personal information in the query and then distributes the encrypted query to the HPs/PBMs functioning as source-entity processors. Ex. 1005, 8:47–9:18, Fig. 4.

In box 5 in Figure 4, an HP/PBM “crunch[es] together” all data items responsive to the parameter list in the query (e.g., including the responsive protected personal information). Ex. 1005, 9:39–51, Fig. 4. Further, the HP/PBM filters out (i.e., eliminates) from the crunched data items all portions that might allow guessing the identity of some data attribute. *Id.* at 9:51–63. Then, the HP/PBM transmits a file to the aggregator processor. *Id.* at 9:64–67.

In boxes 6 and 7 in Figure 4, the aggregator processor agglomerates the responses from the HPs/PBMs to provide “a condensed picture of all of the data” and then reports the results to the marketing team via a user interface. Ex. 1005, 9:24–28, Fig. 4.

2. OVERVIEW OF MURPHY (EXHIBIT 1009)

Murphy is a paper titled “A Security Architecture for Query Tools Used to Access Large Biomedical Databases” by Shawn N. Murphy and Henry C. Chueh in a book titled “Bio*medical Informatics: One Discipline: The Annual Symposium of the American Medical Informatics Association

Proceedings” and edited by Isaac S. Kohane that was publicly accessible in November 2002. Ex. 1005, ix, xviii, 552;⁵ Ex. 1013 ¶¶ 38–45.

Murphy discloses a server application for “data obfuscation” applicable to database query tools for medical information. Ex. 1009, 553. The server application includes an algorithm that blocks the return of search results if the search results relate to fewer than three individuals. *Id.* at 555. Specifically, Murphy explains that the algorithm has “a wider obfuscation at values close to zero” and indicates “the greater range by returning ‘<3’ when the obfuscated number is less than 3.” *Id.*

3. INDEPENDENT CLAIM 7

(a) Limitations 7.a and 7.b

Claim 7 recites a “system” comprising “[7.a] a user computing device [7.b] that produces an encrypted request message for healthcare information that characterizes a group composed of multiple individuals.” Ex. 1001, 11:16–19.

Petitioner contends that Evenhaim teaches limitations 7.a and 7.b because Evenhaim discloses “computers (i.e., computing devices)” in a “system” that includes:

- (1) “a computing device that is called the aggregator” having “a user interface for initiating a query”;
- (2) an aggregator processor that (i) “accepts a query from a user interface” and (ii) “produces a request message for healthcare information that characterizes a group of individuals, e.g., patients, through a ‘parameter list’”; and
- (3) one or more source-entity processors.

⁵ For Exhibit 1009 (Murphy), we follow Petitioner’s practice and cite to the page numbers that appear in the publication.

Pet. 16–17 (citing Ex. 1003 ¶¶ 71–72; Ex. 1005, 6:57–7:2, 7:12–26, 7:59–8:4, 8:30–33, 8:65–9:12, 11:2–5, 14:64–66, 15:3–14, 15:25–45, Fig. 4). According to Petitioner, “the parameter list may include information that characterizes a group of individuals, including, names, dates of birth, common treating physicians, and tracking outcomes of patients in a clinical trial.” *Id.* at 18–19 (citing Ex. 1005, 8:18–22).

Petitioner also contends that Evenhaim “explains that the parameter list in the request is preferably encrypted.” Pet. 17–18 (citing Ex. 1003 ¶ 73; Ex. 1005, 8:47–48, 12:24–34, 13:33–36, 14:4–7).

As noted above, Patent Owner did not file a Preliminary Response. *See supra* § I. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Evenhaim teaches limitations 7.a and 7.b. *See* Pet. 16–19; Ex. 1003 ¶¶ 71–73.

(b) Limitation 7.c

Claim 7 recites “[7.c] the encrypted request message including a unique token produced by the user device for each individual included in the group.” Ex. 1001, 11:19–22.

Petitioner contends that Evenhaim teaches limitation 7.c because Evenhaim discloses that “after the user defines the request, the data aggregator applies an encryption key to encrypt those patients.” Pet. 19 (citing Ex. 1003 ¶ 74; Ex. 1005, Fig. 4 (steps 1–3)). According to Petitioner, an ordinarily skilled artisan would have appreciated that applying an

encryption key to encrypt those patients would create a token for each individual. *Id.*

Further, Petitioner asserts that an ordinarily skilled artisan would have understood that Evenhaim’s token-creation-and-matching system “could be applied to the embodiment in Fig. 4 and 4A such that the aggregator on the user computing device would create encrypted tokens from the list of patients received” in box 3 in Figure 4 to “create the query to the data sources in box 4, and get de-identified patient data back from the data sources in box 6.” Pet. 19 (citing Ex. 1003 ¶¶ 74–78; Ex. 1005, 12:4–13:20).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Evenhaim teaches limitation 7.c. *See* Pet. 19–20; Ex. 1003 ¶¶ 74–78.

(c) Limitation 7.d

Claim 7 recites “[7.d] wherein the user computing device is configured to send the encrypted request message to a server to produce the healthcare information.” Ex. 1001, 11:22–25.

Petitioner contends that Evenhaim teaches limitation 7.d because Evenhaim discloses:

- (1) “a data server called a ‘data source,’ ‘source entity’ or ‘data source entity’ for producing the requested healthcare information”;
- (2) a “data source stores de-identified healthcare records at the patient level (referred to as micro-level data) along with encrypted tokens that can be used to match the data to tokens in a query”; and
- (3) a “data source receives the request message and responds by producing healthcare information,” including “the

de-identified patient records for listed patients, treating physicians, health outcomes, etc.”

Pet. 20–21 (citing Ex. 1003 ¶¶ 79–82; Ex. 1005, 5:11–28, 6:34–45, 6:63–7:27, 8:49–9:12, 10:64–11:2, 12:13–16, 12:36–45, 15:3–14, 15:25–45, 17:53–59, Figs. 4, 4A, 5).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Evenhaim teaches limitation 7.d. *See* Pet. 20–21; Ex. 1003 ¶¶ 79–82.

(d) Limitation 7.e

Claim 7 recites “[7.e] the server is configured to compare the unique request tokens to unique tokens associated with healthcare data to find matching tokens.” Ex. 1001, 11:25–27.

Petitioner contends that Evenhaim teaches limitation 7.e because Evenhaim discloses “request tokens in the form of unique encryption keys” created from personally identifiable information (PII) using “a one-way hash.” Pet. 21 (citing Ex. 1003 ¶ 83; Ex. 1005, 6:64–67, 8:4–13, 8:18–22, 12:27–33, 12:38–42). Further, referring to box 5 in Figure 4, Petitioner asserts that a data server at a data source “compares the query information against the de-identified patient records, which may occur by matching the query tokens to corresponding tokens in a set of de-identified patient records.” *Id.* at 21–22 (citing Ex. 1003 ¶¶ 83–84; Ex. 1005, 12:4–47, 17:27–40).

Petitioner also asserts that an ordinarily skilled artisan would have understood that Evenhaim’s token-creation-and-matching system “could be applied to the embodiment in Fig. 4 and 4A, such that the data sources in box 6 would have de-identified records with encrypted tokens that are

identified in response to a query to the data sources sent in box 4.” Pet. 22 (citing Ex. 1003 ¶¶ 83–84); *see id.* at 22–25.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Evenhaim teaches limitation 7.e. *See* Pet. 19–25; Ex. 1003 ¶¶ 83–85.

(e) Limitation 7.f

Claim 7 recites “[7.f] the unique tokens associated with healthcare data are absent identities of individuals.” Ex. 1001, 11:27–29.

Petitioner contends that Evenhaim teaches limitation 7.f because Evenhaim discloses that “the data sources are careful to encrypt the identifying portions of each record using a common encryption ‘key’” such that “each individual’s healthcare record is de-identified with the token.” Pet. 25–26 (citing Ex. 1003 ¶¶ 86–87; Ex. 1005, 12:8–16, 12:38–45).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Evenhaim teaches limitation 7.f. *See* Pet. 25–26; Ex. 1003 ¶¶ 86–87.

(f) Limitation 7.g

Claim 7 recites “[7.g] the healthcare information being produced based on a minimum number of matched tokens.” Ex. 1001, 11:29–30.

Petitioner contends that the combined disclosures in Evenhaim and Murphy teach limitation 7.g. *See* Pet. 26–27. Specifically, Petitioner asserts that Evenhaim discloses “the inclusion of at least a predetermined minimum number of individuals’ in the search parameters.” *Id.* at 26 (quoting Ex. 1005, 13:62–63). According to Petitioner, an ordinarily skilled artisan would have understood that “requiring a minimum number of individuals corresponds to having a minimum number of tokens used in processing the

query because the tokens correspond to individuals.” *Id.* (citing Ex. 1003 ¶ 88).

Additionally, Petitioner asserts that Murphy discloses “that, in complying with HIPAA, an algorithm preferably blocks the return of search results when doing so would return fewer than three patients, in order to prevent the user from associating a patient with his/her record.” Pet. 26–27. As support, Petitioner quotes Murphy’s disclosure about obfuscating values close to zero as follows: “Therefore, we modify our range algorithm to have a wider obfuscation at values close to zero, and indicate the greater range by returning ‘<3’ when the obfuscated number is less than 3.” *Id.* at 27 (quoting Ex. 1009, 555).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Evenhaim and Murphy teach limitation 7.g. *See* Pet. 26–27; Ex. 1003 ¶¶ 88–90.

(g) Limitation 7.h

Claim 7 recites “[7.h] the identity of the individuals being unattainable from the produced healthcare information.” Ex. 1001, 11:30–32.

Petitioner contends that Evenhaim teaches limitation 7.h because Evenhaim discloses “that the produced healthcare information is absent PII because the data is de-identified.” Pet. 27 (citing Ex. 1003 ¶¶ 91–93; Ex. 1005, 8:49–64, 9:13–18, 10:1–6, 12:12–20, 12:35–44, 14:8–13).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Evenhaim teaches limitation 7.h. *See* Pet. 27; Ex. 1003 ¶¶ 91–93.

(h) Limitations 7.i and 7.j

Claim 7 recites “[7.i] wherein the user computing device is further configured to receive the produced healthcare information to report the characteristics of the group [7.j] absent authorization from the individuals in the group.” Ex. 1001, 11:32–36.

Petitioner contends that Evenhaim teaches limitations 7.i and 7.j because Evenhaim discloses:

- (1) a user computing device “configured to receive a report on the healthcare information of the group,” including “the de-identified medical records themselves, common treating physicians, and outcomes of patients in a clinical trial”; and
- (2) the goal “to produce de-identified healthcare information that can be released to third-parties without individuals in the group authorizing the release, to comply with HIPAA.”

Pet. 27 (citing Ex. 1003 ¶¶ 94–95; Ex. 1005, 3:17–31, 4:34–48, 5:46–6:10, 8:18–22, 8:65–9:12, 10:6–11, 14:7–13, 14:59–67, 15:3–45, Fig. 4); *see id.* at 28.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Evenhaim teaches limitations 7.i and 7.j. *See* Pet. 27–28; Ex. 1003 ¶¶ 94–95.

(i) Alleged Reason to Combine the Teachings of the References

Petitioner identifies a reason that would have prompted an ordinarily skilled artisan to combine Murphy’s teachings with Evenhaim’s teachings in the way Petitioner proposes, i.e., to provide “additional details about how to beneficially implement statistical de-identification.” *See* Pet. 15–16.

Further, Petitioner asserts that an ordinarily skilled artisan would have had a “reasonable expectation of success” in combining the teachings of the references. *Id.* at 16.

Dr. Clark’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 68–70. For instance, Dr. Clark testifies that Murphy describes “measures [that] would prevent a search for a single subject in Evenhaim to result in the identification of the subject’s medical records” and, therefore, “reduc[e] the risk of a HIPAA violation.” *Id.* ¶ 68. According to Dr. Clark, Murphy does so by recommending:

- (1) “at least a minimum amount of de-identified medical data (i.e., multiple patient records) such that the query complies with the HIPAA statistical requirements”; and
- (2) “maintaining a log of queries to ensure that a user does not repeatedly submit a query that returns the same number of results multiple times within a defined time period.”

Id.

Based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would have had a reason, i.e., as articulated by Dr. Clark, to combine Murphy’s teachings with Evenhaim’s teachings in the way Petitioner proposes. *See* Pet. 15–16; Ex. 1003 ¶¶ 68–69. Based on the current record, Petitioner also establishes sufficiently that an ordinarily skilled artisan would have had a reasonable expectation of success in combining the teachings of the references. *See* Pet. 16; Ex. 1003 ¶ 70.

(j) Preliminary Conclusion About Obviousness/Nonobviousness

As discussed above, Petitioner’s analysis addresses how the combined disclosures in Evenhaim and Murphy teach claim 7’s subject matter. *See supra* §§ III.D.3(a)–(h). Moreover, Petitioner provides a reason with

rational underpinning as to why an ordinarily skilled artisan would have been motivated to combine Murphy's teachings with Evenhaim's teachings in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.D.3(i). Hence, Petitioner demonstrates a reasonable likelihood of proving that claim 7 is unpatentable under § 103(a) as obvious over Evenhaim and Murphy.

4. INDEPENDENT CLAIMS 1 AND 14

Claims 1 and 14 recite subject matter similar to claim 7. *Compare* Ex. 1001, 11:16–36 (claim 7), *with id.* at 10:42–63 (claim 1), *and id.* at 12:3–26 (claim 14).

Petitioner contends that the combined disclosures in Evenhaim and Murphy teach claim 1's subject matter and claim 14's subject matter for the reasons that the combined disclosures teach claim 7's subject matter. *See* Pet. 16–28, 32–35. Dr. Clark's testimony supports Petitioner's contentions. *See* Ex. 1003 ¶¶ 71–95, 106–113, 119–128.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark's testimony, Petitioner establishes sufficiently that the combined disclosures in Evenhaim and Murphy teach claim 1's subject matter and claim 14's subject matter. *See* Pet. 16–28, 32–35; Ex. 1003 ¶¶ 71–95, 106–113, 119–128. Additionally, as discussed above, Petitioner provides a reason with rational underpinning as to why an ordinarily skilled artisan would have been motivated to combine Murphy's teachings with Evenhaim's teachings in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.D.3(i). Hence, Petitioner demonstrates a reasonable likelihood of proving that

claims 1 and 14 are unpatentable under § 103(a) as obvious over Evenhaim and Murphy.

5. DEPENDENT CLAIMS 2–6, 8–13, AND 15–20

Claims 2–6 depend directly from claim 1. Ex. 1001, 10:64–11:15.
Claims 8–13 depend directly from claim 7. *Id.* at 11:37–12:2.
Claims 15–20 depend directly from claim 14. *Id.* at 12:27–49.

For claims 2–6, 8–13, and 15–20, Petitioner provides an analysis supported by Dr. Clark’s testimony about how the combined disclosures in Evenhaim and Murphy teach the claimed subject matter. *See* Pet. 28–37; Ex. 1003 ¶¶ 96–105, 114–118, 129–134.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Evenhaim and Murphy teach the subject matter in claims 2–6, 8–13, and 15–20. *See* Pet. 28–37; Ex. 1003 ¶¶ 96–105, 114–118, 129–134. Hence, Petitioner demonstrates a reasonable likelihood of proving that claims 2–6, 8–13, and 15–20 are unpatentable under § 103(a) as obvious over Evenhaim and Murphy.

*E. Alleged Obviousness over Evenhaim,
Settimi, and Murphy: Claims 1–20*

Petitioner contends that claims 1–20 are unpatentable under § 103(a) as obvious over Evenhaim, Settini, and Murphy. *See* Pet. 9, 37–53. Above, we provided overviews of Evenhaim and Murphy. *See supra* §§ III.D.1–III.D.2. Below, we provide an overview of Settini. Then, we consider obviousness issues. As explained below, Petitioner establishes sufficiently for purposes of institution that the combined disclosures in Evenhaim, Settini, and Murphy teach the subject matter in claims 1–20.

1. OVERVIEW OF SETTIMI (EXHIBIT 1006)

Settimi is a U.S. patent application publication titled “Systems and Methods for Identification of Clinical Study Candidates,” filed on November 20, 2006, and published on December 20, 2007. Ex. 1006, codes (12), (22), (43), (54). Settimi states that the invention “relates to identification of clinical study participants based on electronic medical record data.” *Id.* ¶ 4. Referencing HIPAA, Settimi explains that patient data is “sensitive and confidential.” *Id.* ¶ 9. Hence, “any information contained on a medical report or record that could aid in tracing back to a particular individual must be removed from the report or record prior to adding the data to a data warehouse for public data mining.” *Id.*

Settimi’s Figure 2 (reproduced below) depicts an exemplary data warehouse architecture:

FIG. 2

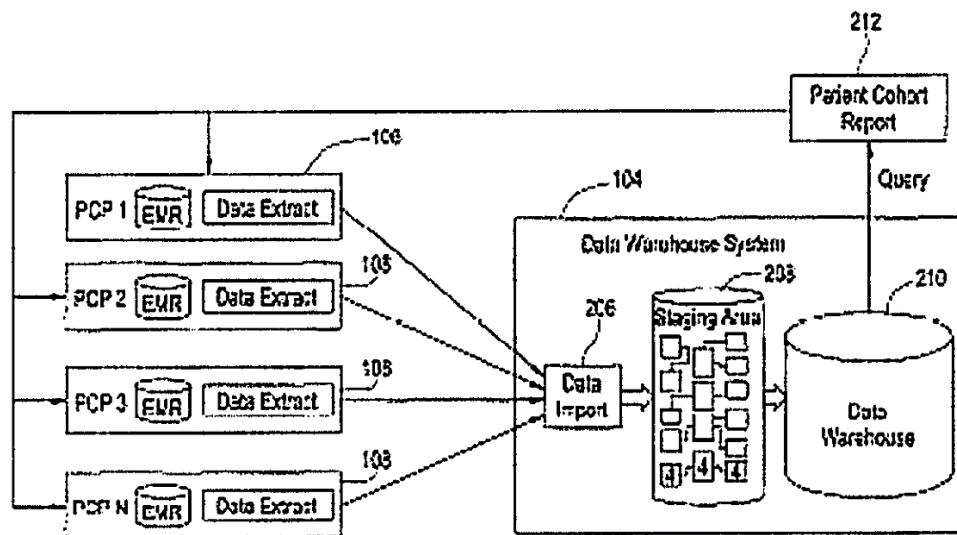


Figure 2 illustrates multiple patient care provider (PCP) systems 108 that provide patient data to data warehouse system 104. Ex. 1006 ¶ 35, Fig. 2.

In Figure 2, each PCP system includes an electronic medical record (EMR) database and “application software for extracting patient data from

the EMR database.” Ex. 1006 ¶ 35, Fig. 2. An “EMR database record includes data such as: patient name and address, medications, allergies, observations, diagnoses, and health insurance information.” *Id.* ¶ 35.

In Figure 2, data warehouse system 104 includes “application software to perform a data import function 206” that “aggregates and cleanses de-identified patient data” from multiple PCP systems 108 and then “stores the data into a staging area 208.” Ex. 1006 ¶ 35, Fig. 2. “Data received from multiple PCP systems 108 is normalized, checked for validity and completeness, and either corrected or flagged as defective.” *Id.* ¶ 35. “Data from multiple PCP systems 108 is then combined together into a relational database” in data warehouse 210 “where it is available for querying.” *Id.* ¶ 35, Fig. 2.

At data warehouse system 104, “the data may be scrubbed and normalized by mapping terms to a common vocabulary.” Ex. 1006 ¶ 60. For instance, “if one record refers to a MI and another record refers to a myocardial infarction, both are coded centrally in the database as a myocardial infarct.” *Id.* Hence, “[a]ggregation, cleaning and staging data in the described fashion allows the data to be queried meaningfully and efficiently.” *Id.* ¶ 35.

A unique identifier associated with each patient record transmitted to data warehouse system 104 allows the system to “connect all records relating to a single patient” and, therefore, permits “querying longitudinal patient data.” Ex. 1006 ¶ 37; *see id.* ¶ 43. “The unique identifier indicates an anonymous or abstract patient having certain characteristics but does not provide personal direct identifying information such as name, social security number, street address, etc.” *Id.* ¶ 37.

Settimi's Figure 3 (reproduced below) depicts an exemplary process for de-identifying patient data during data extraction for transmission to a data warehouse system:

FIG. 3

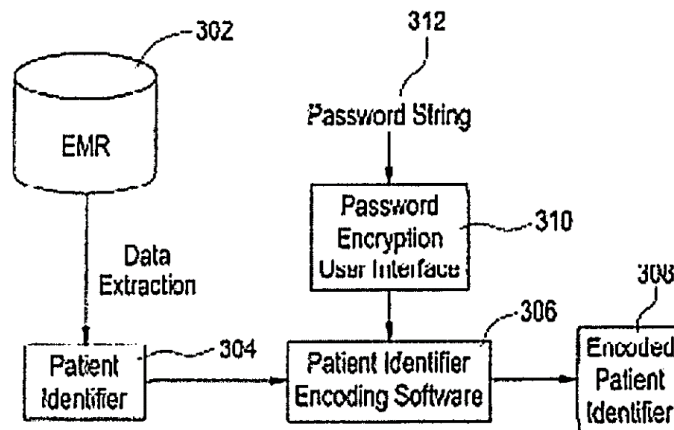


Figure 3 illustrates a de-identification process performed at a PCP system for “remov[ing] information that will identify a patient while still retaining clinically useful information about the patient.” Ex. 1006 ¶¶ 38–39, Fig. 3.

Initially, application software on the PCP system extracts patient data from EMR database 302 and removes patient-identifying information. Ex. 1006 ¶¶ 38–39, Fig. 3. In an exemplary embodiment, the following identifiers, among others, are removed or transformed to create de-identified data: “name, geographic subdivisions smaller than a state including street address, city, county, precinct, zip code (down to the last three digits), dates directly related to an individual (e.g., birth date), phone and fax numbers.” *Id.* ¶ 39.

Each patient record in EMR database 302 includes a patient identifier (PID) 304 “used to uniquely identify an individual patient.” Ex. 1006 ¶ 38, Fig. 3. “The PID 304 is encoded as part of the de-identification process to create an encoded patient identifier (EPID) 308.” *Id.* ¶ 38, Fig. 3.

More particularly, a user at the PCP site supplies password string 312 via password encryption user interface 310 at the PCP site. Ex. 1006, ¶ 41, Fig. 3. Then, encoding software 306 on the PCP system creates EPID 308 based on PID 304 and password string 312. *Id.* ¶ 41, Fig. 3. For example, encoding software 306 hashes password string 312 “to produce a sixteen-digit number” and then adds that sixteen-digit number “to the PID 304 to create the EPID 308.” *Id.* ¶ 41.

After employing Figure 3’s de-identification process, the de-identified patient data in data warehouse system 104 includes “an EPID 308 that may be useful in creating longitudinal reports that analyze more than one record for a particular patient.” Ex. 1006 ¶ 43. Hence, de-identified individuals “may be tracked longitudinally and queried as members of anonymous population cohorts, based on clinical selection criteria,” e.g., to create patient cohort reports. *Id.* ¶ 42; *see id.* ¶¶ 30, 33, 36. An illustrative patient cohort report includes “all patients with a particular disease that were treated with a particular medication.” *Id.* ¶ 36.

2. DIFFERENCES BETWEEN THE CLAIMED INVENTION AND THE PRIOR ART

(a) Independent Claim 7

For claim 7, Petitioner provides an analysis supported by Dr. Clark’s testimony about how the combined disclosures in Evenhaim, Settini, and Murphy teach claim 7’s subject matter. *See* Pet. 40–45; Ex. 1003 ¶¶ 140–162.

As an example, for limitation 7.a requiring “a user computing device,” Petitioner contends that Settini discloses patient care provider (PCP)

systems 108 with PCP user systems comprising personal computers. Pet. 40–41 (citing Ex. 1003 ¶ 140; Ex. 1006 ¶¶ 17, 29, Fig. 7).

As another example, for limitation 7.b requiring that the user device “produce[] an encrypted request message for healthcare information that characterizes a group composed of multiple individuals,” Petitioner contends that Settimi discloses that a PCP user system permits a user to “enter a password string to be used to initiate data extraction and for encrypting a patient identifier.” Pet. 41 (citing Ex. 1003 ¶ 141; Ex. 1006 ¶¶ 29, 41).

As yet another example, for limitation 7.c requiring that “the encrypted request message includ[e] a unique token produced by the user device for each individual included in the group,” Petitioner explains that the proposed combination would employ Settimi’s central data warehouse in Evenhaim’s Figure 4 embodiment with the central data warehouse replacing the HPs/PBMs in Figure 4. Pet. 41. Petitioner also explains that the central data warehouse would store de-identified patient records containing encrypted tokens. *Id.*

Further, Petitioner asserts that an ordinarily skilled artisan would have understood that the encrypted patient list resulting from boxes 3 and 4 in Evenhaim’s Figure 4 would in the proposed combination:

- (1) “use encryption that allows for finding matching records in the central warehouse (e.g., creating a token for each individual in a group in the form of a unique encryption key)”; and
- (2) “be sent to the data source (a central repository with de-identified patient records) that contains corresponding tokens that are matched to determine the relevant healthcare records responsive to the query.”

Pet. 41–43 (citing Ex. 1003 ¶¶ 143–146; Ex. 1005, 12:4–13:20, Figs. 4, 7; Ex. 1006 ¶¶ 35, 37).

As yet another example, for limitation 7.d specifying that the user device “is configured to send the encrypted request message to a server to produce the healthcare information,” Petitioner explains that in the proposed combination Settimi’s central data warehouse includes “a server for producing the requested healthcare information.” Pet. 43 (citing Ex. 1003 ¶ 147; Ex. 1006 ¶¶ 35, 37).

As a further example, for limitation 7.e specifying that the server “is configured to compare the unique request tokens to unique tokens associated with healthcare data to find matching tokens,” Petitioner explains that in the proposed combination Settimi’s central data warehouse “contains de-identified records from the various originating sources,” e.g., from the HPs/PBMs in Evenhaim’s Figure 4. Pet. 43 (citing Ex. 1003 ¶ 149). Petitioner also explains that, according to box 5 in Figure 4, the server at the central data warehouse “matches the query information against the de-identified patient records, matching the produced tokens to corresponding tokens in a set of de-identified patient records.” *Id.* (citing Ex. 1005, 12:4–47). Petitioner asserts that an ordinarily skilled artisan would have understood that “the search would involve matching the tokens sent in the query to the tokens already in the relevant healthcare record.” *Id.* at 43–44 (citing Ex. 1003 ¶ 151).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Evenhaim, Settimi, and Murphy teach claim 7’s subject matter. *See* Pet. 40–45; Ex. 1003 ¶¶ 140–162.

(b) Independent Claims 1 and 14 and
Dependent Claims 2–6, 8–13, and 15–20

For independent claims 1 and 14 and dependent claims 2–6, 8–13, and 15–20, Petitioner provides an analysis supported by Dr. Clark’s testimony about how the combined disclosures in Evenhaim, Settini, and Murphy teach the claimed subject matter. *See* Pet. 45–53; Ex. 1003 ¶¶ 163–199.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Evenhaim, Settini, and Murphy teach the subject matter in claims 1–6 and 8–20. *See* Pet. 45–53; Ex. 1003 ¶¶ 163–199; *supra* § III.E.2(a).

3. ALLEGED REASON TO COMBINE
THE TEACHINGS OF THE REFERENCES

Petitioner identifies a reason that would have prompted an ordinarily skilled artisan to combine Settini’s teachings with the teachings of Evenhaim and Murphy in the way Petitioner proposes, i.e., to employ a central data warehouse that:

- (1) “eliminates the need for conducting searches across different entities”;
- (2) “uses a ‘common vocabulary’ that makes searching easier and more reliable”; and
- (3) “reduc[es] the risk of a HIPAA violation.”

See Pet. 39–40. Further, Petitioner asserts that an ordinarily skilled artisan would have had a “reasonable expectation of success” in combining the teachings of the references. *Id.* at 40.

Dr. Clark’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 137–139. For instance, Dr. Clark testifies that an ordinarily skilled

artisan “would find benefit in applying Settimi’s central database to Evenhaim to streamline, simplify and improve the querying process.” *Id.* ¶ 139.

Based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would have had a reason, i.e., as articulated by Dr. Clark, to combine Settimi’s teachings with the teachings of Evenhaim and Murphy in the way Petitioner proposes. *See* Pet. 39–40; Ex. 1003 ¶¶ 137–139. Based on the current record, Petitioner also establishes sufficiently that an ordinarily skilled artisan would have had a reasonable expectation of success in combining the teachings of the references. *See* Pet. 40; Ex. 1003 ¶ 139.

4. PRELIMINARY CONCLUSION ABOUT OBVIOUSNESS/NONOBVIOUSNESS

As discussed above, Petitioner’s analysis addresses how the combined disclosures in Evenhaim, Settimi, and Murphy teach the subject matter in claims 1–20. *See supra* §§ III.E.2(a)–(b). Additionally, Petitioner provides a reason with rational underpinning as to why an ordinarily skilled artisan would have been motivated to combine Settimi’s teachings with the teachings of Evenhaim and Murphy in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.E.3. Hence, Petitioner demonstrates a reasonable likelihood of proving that claims 1–20 are unpatentable under § 103(a) as obvious over Evenhaim, Settimi, and Murphy.

F. Alleged Obviousness over Dick, Landi, and Murphy: Claims 1–20

Petitioner contends that claims 1–20 are unpatentable under § 103(a) as obvious over Dick, Landi, and Murphy. *See* Pet. 9, 54–75. Above, we

provided an overview of Murphy. *See supra* § III.D.2. Below, we provide overviews of Dick and Landi. Then, we consider obviousness issues. As explained below, Petitioner establishes sufficiently for purposes of institution that the combined disclosures in Dick, Landi, and Murphy teach the subject matter in claims 1–20.

1. OVERVIEW OF DICK (EXHIBIT 1007)

Dick is a U.S. patent application publication titled “Method and Apparatus for Requesting and Retrieving De-Identified Medical Information,” filed on January 23, 2002, and published on August 15, 2002. Ex. 1007, codes (12), (22), (43), (54). Dick states that the invention “relates generally to electronic access of medical information and more specifically to electronic access of medication, pharmaceutical, and clinical information.” *Id.* ¶ 2; *see id.* ¶ 10. The invention “further contemplates the use of ‘de-identifying’ methods and processes for allowing information from the present invention to be distributed for use in medical research.” *Id.* ¶ 13; *see id.* ¶¶ 45–46.

An illustrative method for requesting and retrieving de-identified medical information includes the following steps:

- (1) “receiving a request for medical information including identification of a subject”;
- (2) “transmitting a query to a medical information repository for information pursuant to the request”; and
- (3) “transmitting a response to the request for medical information, including information based on the response to the query.”

Ex. 1007 ¶ 19, code (57), Fig. 1. The “response to the query may be de-identified to remove any identifying information therefrom.” *Id.* at code (57); *see id.* ¶¶ 45–46.

Dick’s Figure 3 (reproduced below) depicts several “physical environments” for accomplishing an illustrative method for requesting and retrieving de-identified medical information:

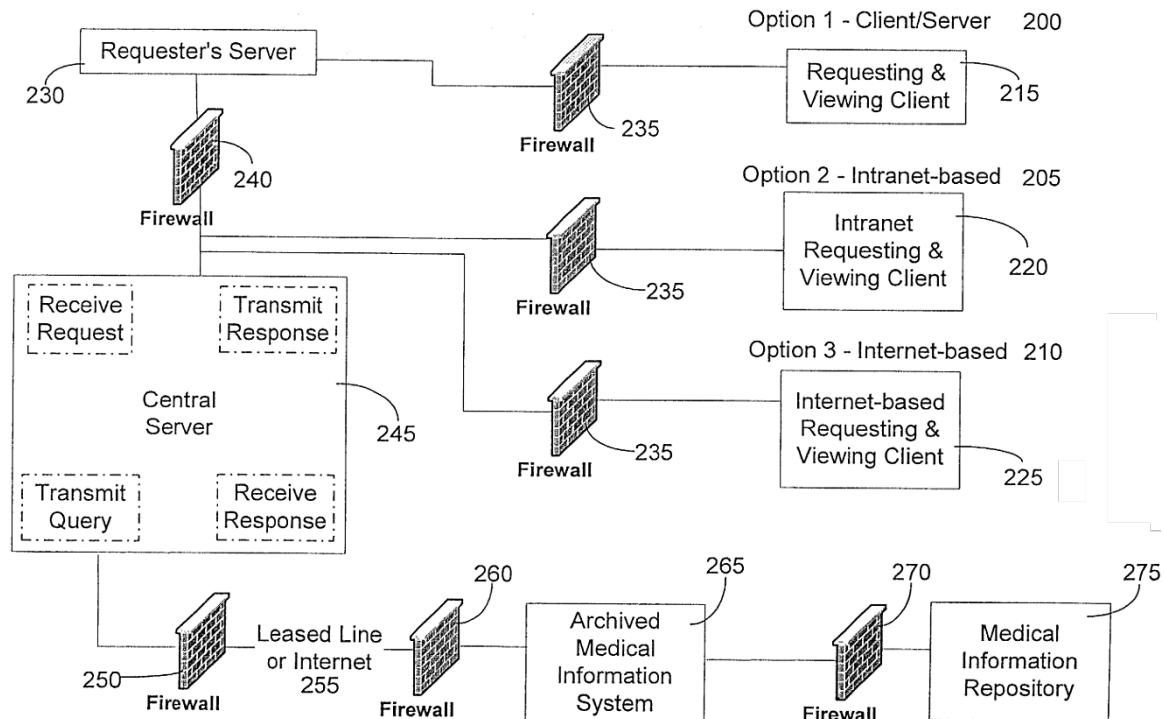


Figure 3 illustrates “three front-end physical environments” as follows:

- (1) “a client-server environment 200”;
- (2) “an intranet-based environment 205”; and
- (3) “an internet-based environment 210.”

Ex. 1007 ¶ 20, Fig. 3; *see id.* ¶¶ 16, 19. “Each front-end physical environment includes one or more requesting and viewing clients (‘RVC’s), respectively, client-server-based 215, intranet-based 220, and internet-based 225.” *Id.* ¶ 20, Fig. 3.

Typically, each RVC is “a terminal having at least a video display and keyboard.” Ex. 1007 ¶ 21. Generally, each RVC is “operated by an authorized user to request and subsequently review retrieved medical information or other search results.” *Id.*

Each request for medical information “includes identification of a subject” that “might consist of a human individual or group of humans.” Ex. 1007 ¶ 24; *see id.* ¶ 40. “The identification of the subject could be by way of name, patient number, social security number, driver’s license number, address, phone number, biometric identification or any other identification or combination of identification characteristics capable of being correlated with stored medical information, if it exists.” *Id.* ¶ 24.

After an RVC receives a request for medical information, “the request is transmitted to and received by a central server 245.” Ex. 1007 ¶ 27, Fig. 3. Then, central server 245 “will transmit a query to a medical information repository 275 for information pursuant to the request.” *Id.* ¶ 28, Fig. 3. Also, central server 245 may access “an Archive Medical Information System (AMIS) server 265.” *Id.* ¶ 28, Fig. 3. “AMIS server 265 may be associated with one or more [medical information repositories] MIRs and may be networked with the MIR to receive data directly from the MIR or may be wholly removed from the MIR, receiving data indirectly.” *Id.* ¶ 30.

“When AMIS server 265 has completed information searches responsive to the query from central server 245, AMIS server 265 will transmit a response to central server 245 conveying the results of the search(es) made pursuant to the query/queries sent by central server 245.” Ex. 1007 ¶ 31. After central server 245 receives a response to the query/

queries, central server 245 prepares a response for the requesting RVC and then sends the response to the requesting RVC. *Id.* ¶¶ 31–32.

2. OVERVIEW OF LANDI (EXHIBIT 1008)

Landi is a U.S. patent titled “Systems and Methods for Encryption-Based De-Identification of Protected Health Information,” filed on March 9, 2004, and issued on April 14, 2009. Ex. 1008, codes (12), (22), (45), (54). Landi states that the invention relates “in general” to “systems and methods for protecting patient privacy when health care information is shared between various healthcare entities” and “in particular” to “systems and methods that implement secured key encryption for de-identifying patient data to ensure patient privacy, while allowing only the owners of the patient data records and/or other legally empowered entities to re-identify subject patients of de-identified data records, when needed.” *Id.* at 1:14–22; *see id.* at 2:30–40, 3:39–48, code (57).

In an “exemplary embodiment of the invention,” a data-processing method includes the following steps:

- (1) “obtaining a data record of an individual which includes individual identifying information”;
- (2) “removing the individual identifying information in the data record to generate a de-identified data record”;
- (3) “generating an encrypted ID for the individual” where “the encrypted ID comprises an encrypted representation of one or more items of individual identifying information”; and
- (4) “storing the encrypted ID with or in the de-identified data record.”

Ex. 1008, 2:41–49. Additionally, “[a] decryption key is securely maintained and accessible by an authorized entity that is legally authorized or

empowered to decrypt the encrypted ID in the de-identified data record to re-identify the individual.” *Id.* at 2:49–53.

A healthcare entity may use “public key/private key pairs” to de-identify and re-identify patient data. Ex. 1008, 4:35–40; *see id.* at 6:61–65, 10:37–42. Moreover, multiple healthcare entities may implement “the same secure public encryption protocol.” *Id.* at 4:65–67; *see id.* at 8:47–55. “The public keys are freely distributable (no HIPAA issues) to healthcare organizations for de-identification of patient data.” *Id.* at 8:47–49.

Each healthcare entity may use “its own public key or both its own public key and [a] master key to encrypt one or more items of patient identifying information contained in the respective patient medical records owned/managed by the healthcare entity), to thereby generate an Encrypted ID for each subject patient.” Ex. 1008, 5:7–13; *see id.* at 6:23–26, 11:3–6. “An Encrypted ID of a given patient is a unique reproducible encrypted version of patient identifying information that is sufficient to uniquely identify the patient.” *Id.* at 5:13–15, 11:7–9; *see id.* at 8:49–55. “[S]ince each Encrypted ID is a unique reproducible encrypted version of patient identifying information, the process preserves patient uniqueness to enable to the same patient to be recognized at different collection times.” *Id.* at 11:23–27; *see id.* at 8:51–55, 10:9–12, 11:27–29.

A healthcare entity may store “each Encrypted ID with or within a corresponding de-identified data patient data record (i.e., a patient data records [sic] from which patient identifying information has been removed).” Ex. 1008, 5:32–36; *see id.* at 5:36–41, 6:26–27. A healthcare entity may transfer de-identified patient data records to a central patient

data processing system comprising “a repository of persistently stored de-identified patient data records” containing “de-identified (encrypted) patient identifying information, which are collected from the different clinical sites.” *Id.* at 5:44–47, 7:3–7; *see id.* at 14:26–29.

3. INDEPENDENT CLAIM 7

(a) Limitations 7.a and 7.b

Claim 7 recites a “system” comprising “[7.a] a user computing device [7.b] that produces an encrypted request message for healthcare information that characterizes a group composed of multiple individuals.” Ex. 1001, 11:16–19.

Petitioner contends that Dick teaches limitation 7.a and that the combined disclosures in Dick and Landi teach limitation 7.b. *See* Pet. 59–61. Specifically, Petitioner asserts that Dick discloses different types of requesting and viewing clients (RVCs) including a client-server RVC that is “a terminal having at least a video display and keyboard.” *Id.* at 59–60 (citing Ex. 1007 ¶¶ 20–21). Petitioner asserts that Dick’s client-server RVC “allow[s] a user to ‘request and subsequently review retrieved medical information’ that characterizes a ‘subject’ who may be ‘a human individual or group of humans.’” *Id.* at 60 (quoting Ex. 1007 ¶¶ 21, 24) (citing Ex. 1007 ¶¶ 21–22, 44–46, code (57), claim 23, Figs. 1–3).

Additionally, Petitioner contends that an ordinarily skilled artisan would have combined “Landi’s central database of de-identified medical records, which contain associated Encryption IDs created with freely distributable public keys, with Dick’s system for searching a central database for a ‘group’ of individuals.” Pet. 60 (citing Ex. 1007 ¶¶ 11, 24–25); *see id.* at 57–58. Petitioner explains that an ordinarily skilled artisan

would have used a public key according to Landi’s method to “create the list of Encrypted IDs” on Dick’s client-server RVC for querying the central database. *Id.* at 60 (citing Ex. 1003 ¶¶ 213–214; Ex. 1007 ¶¶ 11, 19). According to Petitioner, “creat[ing] the list of Encrypted IDs” on Dick’s client-server RVC “would minimize the transmission of PII and further ensure compliance with HIPAA.” *Id.* at 60–61.

As noted above, Patent Owner did not file a Preliminary Response. *See supra* § I. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Dick teaches limitation 7.a and that the combined disclosures in Dick and Landi teach limitation 7.b. *See* Pet. 59–61; Ex. 1003 ¶¶ 211–215.

(b) Limitation 7.c

Claim 7 recites “[7.c] the encrypted request message including a unique token produced by the user device for each individual included in the group.” Ex. 1001, 11:19–22.

Petitioner contends that the combined disclosures in Dick and Landi teach limitation 7.c. *See* Pet. 61–62. Specifically, Petitioner asserts that Dick’s client-server RVC:

- (1) “receives a request from a user for medical records for a ‘subject’ that may be ‘a human individual or group of humans’”; and
- (2) sends the request to “a repository containing associated medical records.”

Id. at 61 (quoting Ex. 1007 ¶ 24) (citing Ex. 1003 ¶ 215; Ex. 1007 ¶¶ 11, 19, 22–24, 44–46, code (57), claim 23, Figs. 1–3).

Petitioner asserts that Landi discloses a central patient data processing system containing “solely de-identified records in which PII has been replaced with a token in the form of Encrypted IDs for each individual that has patient records.” Pet. 61 (citing Ex. 1003 ¶¶ 216–217; Ex. 1008, 4:40–46, 11:23–29).

Further, Petitioner asserts that an ordinarily skilled artisan would have employed Landi’s token-creation-and-matching system with Dick’s system such that Dick’s client-server RVC would “query de-identified patient records held on a data server (Medical Information Repository in Dick and/or central repository in Landi) using the public encryption key from Landi to create encrypted tokens to be used for such requests.” Pet. 62 (citing Ex. 1003 ¶¶ 218–220; Ex. 1008, 8:49–52).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Dick and Landi teach limitation 7.c. *See* Pet. 61–62; Ex. 1003 ¶¶ 216–221.

(c) Limitation 7.d

Claim 7 recites “[7.d] wherein the user computing device is configured to send the encrypted request message to a server to produce the healthcare information.” Ex. 1001, 11:22–25.

Petitioner contends that the combined disclosures in Dick and Landi teach limitation 7.d. *See* Pet. 62–63. Specifically, Petitioner asserts that Dick’s client-server RVC “receives a request for an authorized user for medical information” and then sends the request to “a central server.” *Id.* at 62 (citing Ex. 1007 ¶¶ 22, 27). Petitioner asserts that Landi’s central patient data processing system includes “a data server” because “it is a

networked computer system that stores de-identified medical records for the purpose of sharing in response to third-party queries.” *Id.* at 63 (citing Ex. 1003 ¶ 222; Ex. 1008, 7:3–31, 8:16–55, 10:52–65).

Further, Petitioner asserts that an ordinarily skilled artisan would have employed Landi’s token-creation-and-matching system with Dick’s system such that Dick’s client-server RVC would “convert the query in Dick to tokens” because that would “minimize the transmission of PII and further ensure compliance with HIPAA.” Pet. 63 (citing Ex. 1003 ¶ 221). Petitioner explains that “[a]fter the query is encrypted” in the proposed combination, the encrypted query “is transmitted to a medical information repository and the central server prepares a response to the request to produce the information contained in the request.” *Id.* (citing Ex. 1007 ¶¶ 27–28, 32, Fig. 3).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Dick and Landi teach limitation 7.d. *See* Pet. 62–63; Ex. 1003 ¶¶ 222–223.

(d) Limitation 7.e

Claim 7 recites “[7.e] the server is configured to compare the unique request tokens to unique tokens associated with healthcare data to find matching tokens.” Ex. 1001, 11:25–27.

Petitioner contends that the combined disclosures in Dick and Landi teach limitation 7.e. *See* Pet. 63–65. Petitioner explains that tokens in queries sent from Dick’s client-server RVC to Dick’s central server would in the proposed combination “correspond to the similarly encrypted tokens in the de-identified patient records in the medical information repository” (data

server) in Landi’s central patient data processing system. *Id.* at 63.

According to Petitioner, “Landi explains that the tokens in the de-identified records in the central system/database” are “used to recognize (i.e., identify) the records that match the corresponding tokens created by encrypting the same patient information elsewhere using the common public key.” *Id.* at 64–65 (citing Ex. 1003 ¶ 223; Ex. 1008, 8:38–55, 11:23–29, 11:52–63).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Dick and Landi teach limitation 7.e. *See* Pet. 63–65; Ex. 1003 ¶ 224.

(e) Limitation 7.f

Claim 7 recites “[7.f] the unique tokens associated with healthcare data are absent identities of individuals.” Ex. 1001, 11:27–29.

Petitioner contends that Landi teaches limitation 7.f because Landi discloses that “the produced healthcare information is absent PII because the healthcare information can be produced to third parties without compromising the patient privacy.” Pet. 65 (citing Ex. 1003 ¶¶ 224–225; Ex. 1008, 2:5–26, 2:30–54, 5:32–47, 13:41–53).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Landi teaches limitation 7.f. *See* Pet. 65; Ex. 1003 ¶¶ 225–226.

(f) Limitation 7.g

Claim 7 recites “[7.g] the healthcare information being produced based on a minimum number of matched tokens.” Ex. 1001, 11:29–30.

Petitioner contends that the combined disclosures in Dick and Murphy teach limitation 7.g. *See* Pet. 65. Specifically, Petitioner asserts that Dick

discloses “using statistical methods to ensure that an individual’s medical records are not identified.” *Id.* (citing Ex. 1003 ¶¶ 226–228; Ex. 1007 ¶ 46). Petitioner asserts that “Murphy makes clear that, in complying with HIPAA, an algorithm preferably blocks the return of search results when doing so would return fewer than three patients, in order to prevent the user from associating a patient with his/her record.” *Id.* (citing Ex. 1003 ¶ 229; Ex. 1009, 555).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Dick and Murphy teach limitation 7.g. *See* Pet. 65; Ex. 1003 ¶¶ 227–230.

(g) Limitation 7.h

Claim 7 recites “[7.h] the identity of the individuals being unattainable from the produced healthcare information.” Ex. 1001, 11:30–32.

Petitioner contends that Landi teaches limitation 7.h because Landi’s Encrypted IDs “prevent identification of the individuals.” Pet. 65 (citing Ex. 1008, 7:22–30, 11:13–17). According to Petitioner, “Landi explains that the public key allows for encryption of the PII, but does not allow for decryption—only the private key (which is not disseminated) allows for decryption.” *Id.* at 65–66 (citing Ex. 1003 ¶¶ 230–232; Ex. 1008, 4:35–48, 5:2–31, 7:34–38, 11:13–19).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Landi teaches limitation 7.h. *See* Pet. 65–66; Ex. 1003 ¶¶ 231–233.

(h) Limitations 7.i and 7.j

Claim 7 recites “[7.i] wherein the user computing device is further configured to receive the produced healthcare information to report the characteristics of the group [7.j] absent authorization from the individuals in the group.” Ex. 1001, 11:32–36.

Petitioner contends that Dick teaches limitation 7.i and that the combined disclosures in Dick and Landi teach limitation 7.j. *See* Pet. 66–68. Specifically, Petitioner asserts that:

- (1) Dick discloses that a client-server RVC “receive[s] a report on the characteristics of the group in response to the query made from the user’s request”;
- (2) Dick discloses “producing healthcare information without the individuals in the group having authorized production”; and
- (3) Landi discloses “produc[ing] healthcare information without the individuals in the group having authorized production in that the very purpose of Landi’s system is to comply with the HIPAA requirements for such disclosure.”

Id. at 66–67 (citing Ex. 1003 ¶¶ 233–234; Ex. 1007 ¶¶ 24, 26, 32, 47, Fig. 1; Ex. 1008, 1:5–18).

Further, Petitioner asserts that an ordinarily skilled artisan “would have appreciated that the purpose of de-identification in Dick and Landi is to be able to disclose healthcare records without patient authorization.” Pet. 68 (citing Ex. 1003 ¶ 235).

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Dick teaches limitation 7.i and that the combined disclosures in Dick and Landi teach limitation 7.j. *See* Pet. 66–68; Ex. 1003 ¶¶ 234–236.

(i) Alleged Reasons to Combine the Teachings of the References

Petitioner identifies reasons that would have prompted an ordinarily skilled artisan to combine Landi’s teachings and Murphy’s teachings with Dick’s teachings in the way Petitioner proposes. *See* Pet. 55–59, 61–62. Further, Petitioner asserts that an ordinarily skilled artisan would have had a “reasonable expectation of success” in combining the teachings of the references. *Id.* at 58–59.

Dr. Clark’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 201–210, 220–221, 230. For instance, Dr. Clark testifies that “Dick describes or suggests de-identification for complying with HIPAA” but “does not describe any specific method to use for this de-identification.” *Id.* ¶ 202 (citing Ex. 1007 ¶¶ 13, 46). Therefore, according to Dr. Clark, an ordinarily skilled artisan “relying on Dick” would have looked to “other sources to implement the de-identification called for in Dick.” *Id.*

Regarding the Dick-Landi combination, Dr. Clark explains how Landi’s teachings comport with Dick’s teachings as follows:

Landi’s detailed disclosure on how to create encrypted tokens from identifying information using the same or similar public encryption keys fits perfectly into Dick’s system for producing de-identified healthcare information that characterizes a group of individuals, and would work well for accomplishing the examples described in Dick, such as querying for healthcare information based on identifying information in order to do risk analysis, while complying with HIPAA.

Ex. 1003 ¶ 207.

Further, Dr. Clark testifies that an ordinarily skilled artisan would have looked to “combine Dick and Landi with Murphy because Murphy provides additional information about protecting the identity of individuals

by preventing their identity from being revealed when a parameter-based search is performed on a medical database in compliance with HIPAA.” Ex. 1003 ¶ 208. Dr. Clark explains that “Murphy describes an algorithm which blocks queries that return fewer than 3 patients thereby preventing disclosing the patient’s identity.” *Id.* ¶ 209.

Based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would have had reasons to combine Landi’s teachings and Murphy’s teachings with Dick’s teachings in the way Petitioner proposes. *See* Pet. 55–59, 61–62; Ex. 1003 ¶¶ 201–209, 220–221, 230. Based on the current record, Petitioner also establishes sufficiently that an ordinarily skilled artisan would have had a reasonable expectation of success in combining the teachings of the references. *See* Pet. 58–59; Ex. 1003 ¶¶ 207, 210, 221, 230.

(j) Preliminary Conclusion About Obviousness/Nonobviousness

As discussed above, Petitioner’s analysis addresses how the combined disclosures in Dick, Landi, and Murphy teach claim 7’s subject matter. *See supra* §§ III.F.3(a)–(h). Moreover, Petitioner provides reasons with rational underpinnings as to why an ordinarily skilled artisan would have been motivated to combine Landi’s teachings and Murphy’s teachings with Dick’s teachings in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.F.3(i). Hence, Petitioner demonstrates a reasonable likelihood of proving that claim 7 is unpatentable under § 103(a) as obvious over Dick, Landi, and Murphy.

4. INDEPENDENT CLAIMS 1 AND 14

Claims 1 and 14 recite subject matter similar to claim 7. *Compare* Ex. 1001, 11:16–36 (claim 7), *with id.* at 10:42–63 (claim 1), *and id.* at 12:3–26 (claim 14).

Petitioner contends that the combined disclosures in Dick, Landi, and Murphy teach claim 1’s subject matter and claim 14’s subject matter for the reasons that the combined disclosures teach claim 7’s subject matter. *See* Pet. 59–68, 70–74. Dr. Clark’s testimony supports Petitioner’s contentions. *See* Ex. 1003 ¶¶ 211–236, 241–248, 254–263.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Dick, Landi, and Murphy teach claim 1’s subject matter and claim 14’s subject matter. *See* Pet. 59–68, 70–74; Ex. 1003 ¶¶ 211–236, 241–248, 254–263. Additionally, as discussed above, Petitioner provides reasons with rational underpinnings as to why an ordinarily skilled artisan would have been motivated to combine Landi’s teachings and Murphy’s teachings with Dick’s teachings in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.F.3(i). Hence, Petitioner demonstrates a reasonable likelihood of proving that claims 1 and 14 are unpatentable under § 103(a) as obvious over Dick, Landi, and Murphy.

5. DEPENDENT CLAIMS 2–6, 8–13, AND 15–20

Claims 2–6 depend directly from claim 1. Ex. 1001, 10:64–11:15. Claims 8–13 depend directly from claim 7. *Id.* at 11:37–12:2. Claims 15–20 depend directly from claim 14. *Id.* at 12:27–49.

For claims 2–6, 8–13, and 15–20, Petitioner provides an analysis supported by Dr. Clark’s testimony about how the combined disclosures in Dick, Landi, and Murphy teach the claimed subject matter. *See* Pet. 68–72, 74–75; Ex. 1003 ¶¶ 237–240, 249–253, 264–269.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Dick, Landi, and Murphy teach the subject matter in claims 2–6, 8–13, and 15–20. *See* Pet. 68–72, 74–75; Ex. 1003 ¶¶ 237–240, 249–253, 264–269. Hence, Petitioner demonstrates a reasonable likelihood of proving that claims 2–6, 8–13, and 15–20 are unpatentable under § 103(a) as obvious over Dick, Landi, and Murphy.

IV. CONCLUSION

Based on the arguments and evidence presented, we determine that there is a reasonable likelihood Petitioner would prevail with respect to at least one claim challenged in the Petition. Hence, we institute an *inter partes* review of all challenged claims on all challenges included in the Petition. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1355 (2018) (noting that the language of 35 U.S.C. § 314(b) “indicates a binary choice—either institute review or don’t”); *PGS Geophysical AS v. Iancu*, 891 F.3d 1354, 1360 (Fed. Cir. 2018) (interpreting the statute as requiring “a simple yes-or-no institution choice respecting a petition, embracing all challenges included in the petition”); 37 C.F.R. § 42.108(a).

At this preliminary stage, we have not made a final determination about the patentability of any challenged claim, the construction of any claim term, phrase, or limitation, or any other legal or factual issue.

V. ORDER

Accordingly, it is

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–20 in the '012 patent is instituted on all challenges included in the Petition; and

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

IPR2024-00381
Patent 10,886,012 B1

For PETITIONER:

Justin J. Oliver
Nicholas Marcello
Michael P. Sandonato
VENABLE LLP
JOliver@Venable.com
NDMarcello@Venable.com
MSandonato@Venable.com

For PATENT OWNER:

W. Karl Renner
Jeffrey J. Barclay
Nicholas W. Stephens
FISH & RICHARDSON P.C.
axf-ptab@fr.com
renner@fr.com
barclay@fr.com
nstephens@fr.com