

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DATAVANT, INC.,
Petitioner,

v.

VIGILYTICS LLC,
Patent Owner.

IPR2024-00307
Patent 9,965,651 B1

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

McNAMARA, *Administrative Patent Judge*.

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

I. INTRODUCTION

Datavant, Inc. (“Petitioner”) filed a petition, Paper 1 (“Petition” or “Pet.”), to institute an *inter partes* review (“IPR”) of claims 1–20 (the “challenged claims”) of U.S. Patent No. 9,965,651 (Ex. 1001, “the ’651 patent”). 35 U.S.C. § 311. Vigilytics LLC (“Patent Owner”) did not file a Preliminary Response. We have jurisdiction under 35 U.S.C. § 6. An *inter partes* review may not be instituted unless the information presented in the Petition “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 decision to institute under § 314 may not institute on fewer than all claims challenged in the petition. *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018). In addition, per Board practice, if the Board institutes trial, it will institute “on all of the challenged claims and on all grounds of unpatentability asserted for each claim.” *See* 37 C.F.R. § 42.108(a) (2023).

Having considered the arguments and the associated evidence presented in the Petition, for the reasons described below, we institute *inter partes* review.

II. REAL PARTIES IN INTEREST

The Petition identifies Datavant, Inc. and Ciox Health LLC as real parties-in-interest. Pet. 1. Patent Owner identifies itself (Vigilytics LLC) as a real party-in-interest. Paper 3, 1.

III. RELATED MATTERS

Patent Owner states that the ’651 patent is involved in the following litigation:

Milliman, Inc. et al. v. Gradient AI Corp. et. al., No. 1:21-cv-10865 (D. Mass.), (“the Milliman Litigation”). Paper 3, 1.

IV. THE '651 PATENT

The '651 patent is titled “Using De-Identified Data to Evaluate Post-Healthcare Facility Encounter Treatment Outcomes.” Ex. 1001, code (54). The patent “relates to processing and transmitting personal data, the dissemination of which is restricted by federal law.” *Id.* at 1:25–27. Specifically, the patent relates to “de-identifying patient identities from healthcare facility encounters and retrieving information from pre or post encounter activity.” *Id.* at 1:60–62.

The patent discloses a computer-implemented method for “producing medical information from a set of private data representing pre or post-encounter characteristics of the individuals, where the individuals have had an encounter with a healthcare facility.” Ex. 1001, 1:64–67. The identity of the individuals is unattainable from the produced information. *Id.* at 1:67–2:1. The method also includes providing the produced information to report the post-encounter characteristics of the group. *Id.* at 2:1–3.

This operation is illustrated in Figure 3 of the '651 patent, reproduced below.

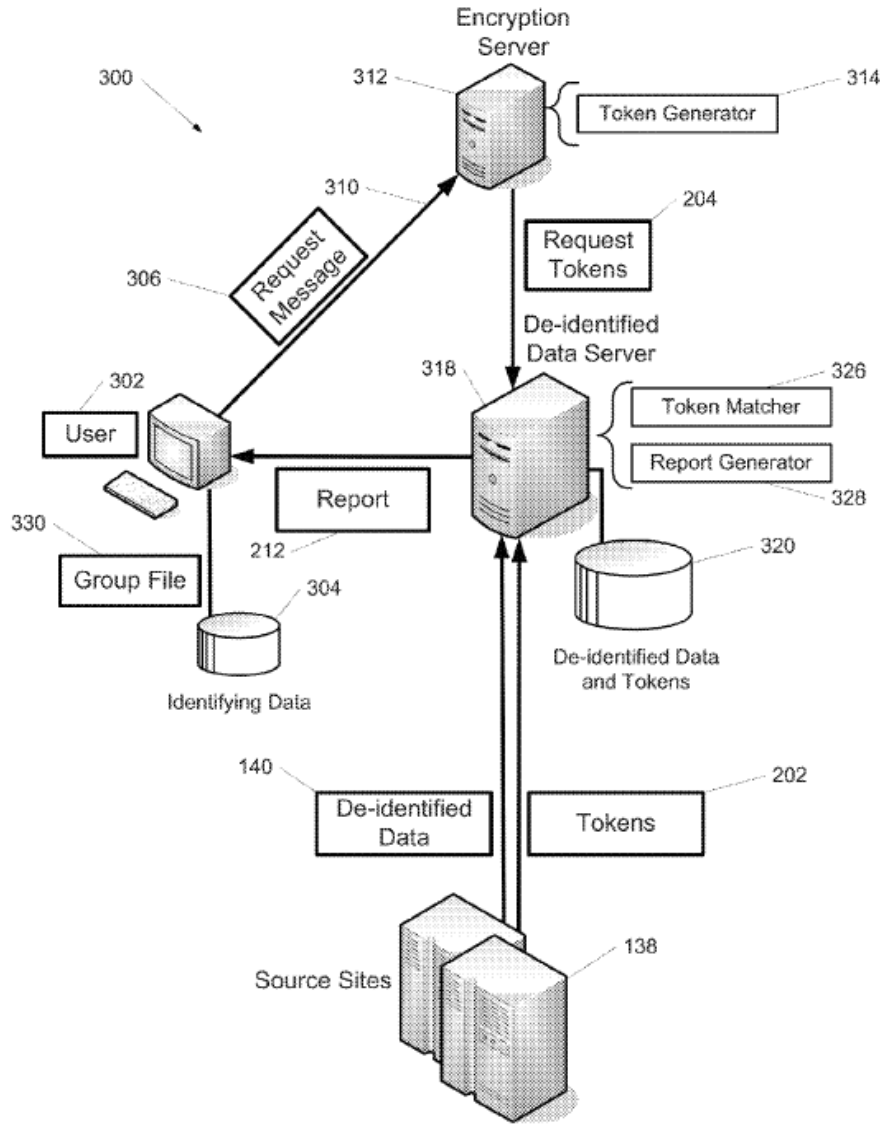


Figure 3 “illustrates an exemplary system incorporating an encryption server and a de-identified data server to enable a user who is not permitted to obtain the private data of a group of individuals who have been discharged from a hospital to instead obtain a report that characterizes the group of discharges as a whole.” Ex. 1001, 3:45–50. In operation, request message 306 is sent over communications network 310 (e.g., the Internet) to encryption server 312. *Id.* at 6:29–31. If request message 306 contains a minimum number of group members, encryption server 312 creates a unique token, or identifier, for each person in request message 306. *Id.* at 6:31–34.

The encryption server creates each token by applying token generator 314 that encrypts the personally identifiable information of each group member. Ex. 1001, 6:34–37. A minimum number of group members, for example ten, is chosen to make it effectively impossible to associate individual group members with individual tokens in the batch of request tokens 204. *Id.* at 6:40–43.

Encryption server 312 provides request tokens 204 to de-identified data server 318. Ex. 1001, 6:44–45. De-identified data server 318 stores records of de-identified data and corresponding tokens 320 obtained from source sites 138 such as pharmacies, healthcare professionals and electronic claims clearing houses. *Id.* at 6:45–49. Each token obtained from the source sites 138 may have been created using the same token generator 314 used by the encryption server 312, or using any other means that generates the identical token for the same personally identifiable information. *Id.* at 6:54–58.

Token matcher 326 performs a look-up in de-identified database 320 to find all tokens that match the tokens sent from encryption server 312. Ex. 1001, 7:6–9. All available data for matched tokens, the requested de-identified data 208, is retrieved for use in report generator 328. *Id.* at 7:9–11.

V. ILLUSTRATIVE CLAIMS

Claims 1, 7, and 14 are independent. Petitioner cites system claim 7 as illustrative of the subject matter claimed in the '651 patent. Independent claim 7 is reproduced below using the claim limitation designations in the Petition:

- [7.a] A system comprising: a computing device comprising: a memory configured to store instructions; and a processor to execute the instructions to perform operations comprising:
- [7.b] receiving a request from a user device for information that characterizes a group composed of multiple individuals
- [7.c] from a set of de-identified data representing characteristics of the individuals pre-or post-encounter with a healthcare facility,
- [7.d] wherein the request contains identifying data for each member in the group of multiple individuals who have had an encounter with a healthcare facility;
- [7.e] producing, by a hardware processor, a request token for each individual included in the group of individuals;
- [7.f] comparing the request tokens to tokens associated with the medical data to find matching tokens
- [7.g] and to determine whether the group includes at least a minimum number of individuals to be included in a report in response to the request
- [7.h] wherein the minimum number of individuals are selected according to at least a privacy-preserving rule that disallows same individuals to be included within a defined period of time;
- [7.i] producing the requested information that characterizes the group,
- [7.j] an identity of the individuals being unattainable from the produced information;
- [7.k] and providing the produced medical information to report the characteristics of the group of individuals
- [7.l] absent authorization from the individuals in the group of individuals identified in the request containing identifying data.

See Pet. iv. Independent claim 1 is a method claim that recites steps corresponding to the operations carried out by the system recited in claim 7.

See Ex. 1001, 12:16–42. Independent claim 14 is drawn to a computer readable storage device that stores instructions executable by a processing

device to carry out operations that correspond to the operations and steps recited in claims 1 and 7. *See id.* at 13:43–14:24.

VI. ASSERTED GROUNDS

Petitioner asserts that claims 1–20 would be unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–20	103 ¹	Evenhaim, ² Murphy ³
1–20	103	Evenhaim, Settimi, ⁴ Murphy
1–20	103	Dick, ⁵ Landi, ⁶ Murphy

In support of its challenges, Petitioner also cites the Declaration of Dr. Paul Clark (“Ex. 1003, Clark Decl.”).

VII. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner identifies a person of ordinary skill in the art (“POSA” or “ordinarily skilled artisan”) as having “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

¹ The Leahy-Smith America Invents Act (“AIA”) included revisions to 35 U.S.C. § 103 that became effective on March 16, 2013. The ’651 patent issued from a continuation application filed on May 26, 2017 (Ex. 1001, code (22)), which is a continuation of applications filed on April 22, 2016 and November 18, 2013, and claims priority under 35 U.S.C. § 120 as a continuation-in-part to an application filed on June 30, 2010. *Id.* at code (63), 1:7–21. Therefore, we apply the pre-AIA version of the statutory basis for unpatentability.

² U.S. Pat. No. 7,823,207 (Ex. 1005)

³ Murphy and Church, “A Security Architecture for Query Tools Used to Access Large Biomedical Databases,” in *Bio*medical Informatics: One Discipline, AMIA 2002 Symposium Proceedings* 552–56 (Isaac S. Kohane, ed., 2002) (Ex. 1009)

⁴ U.S. Pat. Appl. Publ. No. US 2007/0294111 (Ex. 1006)

⁵ U.S. Pat. Appl. Publ. No. US 2002/0111833 (Ex. 1007)

⁶ U.S. Pat. No. 7,519,591 (Ex. 1008)

networking and/or data records management.” Pet. 8. Petitioner further states that “[s]uperior education could compensate for less work experience, and vice-versa.” *Id.* at 8–9 (citing Ex. 1003, Clark Decl. ¶¶ 22–25).

The level of ordinary skill in the art usually is evidenced by the references themselves. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978). For purposes of this Decision, we apply Petitioner’s description of a person of ordinary skill in the art, because it appears commensurate with the subject matter of the ’651 patent and the references.

VIII. CLAIM CONSTRUCTION

We interpret claim terms 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). In this context, claim terms “are generally given their ordinary and customary meaning” as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). “In determining the meaning of the disputed claim limitation, we look 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). Extrinsic evidence is “less significant than the intrinsic record in determining ‘the legally operative meaning of claim language.’” *Phillips*, 415 F.3d at 1317.

Any special definition for a claim term must be set forth in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

“The Board is required to construe ‘only those terms ... that are in controversy, and only to the extent necessary to resolve the controversy.’” *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) (alteration in original).

Petitioner proposes and the Petition applies the claim constructions proposed by Patent Owner in the Milliman Litigation, as shown in the following table:

Term	Construction
Token	An identifier associated with an individual that does not reveal the identity of the individual
Server	A computer, with a processor and memory, on a network that provides information in response to requests from another computer
Similarly encrypted	Generated such that tokens generated from corresponding information can be compared to one another to detect a match
Medical information	Plain and ordinary meaning that includes information about history of physician visits, medical conditions, procedures performed, prescriptions or disabilities

Pet. 7–8.

Petitioner expressly “adopts these constructions for this proceeding” Pet. 7. We understand these constructions to be Petitioner’s identification of “[h]ow the challenged claim is to be construed” under the *Phillips* standard applied by the district courts. 37 C.F.R. §§ 42.100(b), 42.104(b)(4) (2019). Without a Patent Owner Preliminary Response, we are not in a position to determine which constructions, if any, are necessary and disputed. *Vivid Techs., Inc.*, 200 F.3d at 803; *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Nevertheless, at this

stage, we determine that no claim term requires an explicit construction to decide whether Petitioner satisfies the “reasonable likelihood” standard for instituting trial.

IX. ANALYSIS

A. Introduction

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

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. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of “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) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)); *see In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016) (citing *DyStar*

Textilfarben GmbH & Co. Deutschland KG v. C. H. Patrick Co., 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

An obviousness analysis “need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” *KSR*, 550 U.S. at 418; *accord In re Translogic Tech., Inc.*, 504 F.3d 1249, 1259 (Fed. Cir. 2007). Petitioner cannot satisfy its burden of proving obviousness by employing “mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Instead, Petitioner must articulate a reason why a person of ordinary skill in the art would have combined the prior-art references. *In re NuVasive*, 842 F.3d 1376, 1382 (Fed. Cir. 2016).

A reason to combine or modify the prior art may be found explicitly or implicitly in market forces; design incentives; the “interrelated teachings of multiple patents”; “any need or problem known in the field of endeavor at the time of invention and addressed by the patent”; and the background knowledge, creativity, and common sense of the person of ordinary skill. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418–21 (2007)).

In determining whether a claim is obvious in light of the prior art, when in evidence, we consider any relevant objective evidence of non-obviousness. *See Graham*, 383 U.S. at 17. Notwithstanding what the teachings of the prior art would have suggested to one of ordinary skill in the art at the time of the invention, the totality of the evidence submitted, including objective evidence of non-obviousness, may lead to a conclusion that the challenged claims would not have been obvious to one of ordinary skill. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). At this stage

of the proceeding Patent Owner does not present evidence of such objective considerations.

We analyze the asserted grounds of unpatentability in accordance with these principles to determine whether Petitioner has met its burden to establish a reasonable likelihood of success at trial.

B. Petitioner’s Contentions That Claims 1–20 Are Unpatentable as Obvious over Evenhaim and Murphy

1. Evenhaim (Ex. 1005)

Evenhaim is titled “Privacy Preserving Data Mining Protocol.” Ex. 1005, code (54). Evenhaim addresses a “data privacy paradox.” *Id.* at 1:51–52. 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.” *Id.* at 1:54–58. “The Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the USA and similar legislation in other jurisdictions prevents HMOs and healthcare providers from sharing data at full transparency—since the privacy of individuals must be preserved.” *Id.* at 1:58–62. According to Evenhaim, “this data privacy paradox prohibits making best use of the information—especially for applications that are not concerned with any particular John Doe.” *Id.* at 1:51–54.

To address this “paradox,” Evenhaim discloses a protocol for “allowing higher resolution query and manipulation of privacy sensitive data while simultaneously not allowing individual privacy to be breached.” Ex. 1005, 6:49–56.

Evenhaim's Figure 4, reproduced below, illustrates its approach to this paradox.

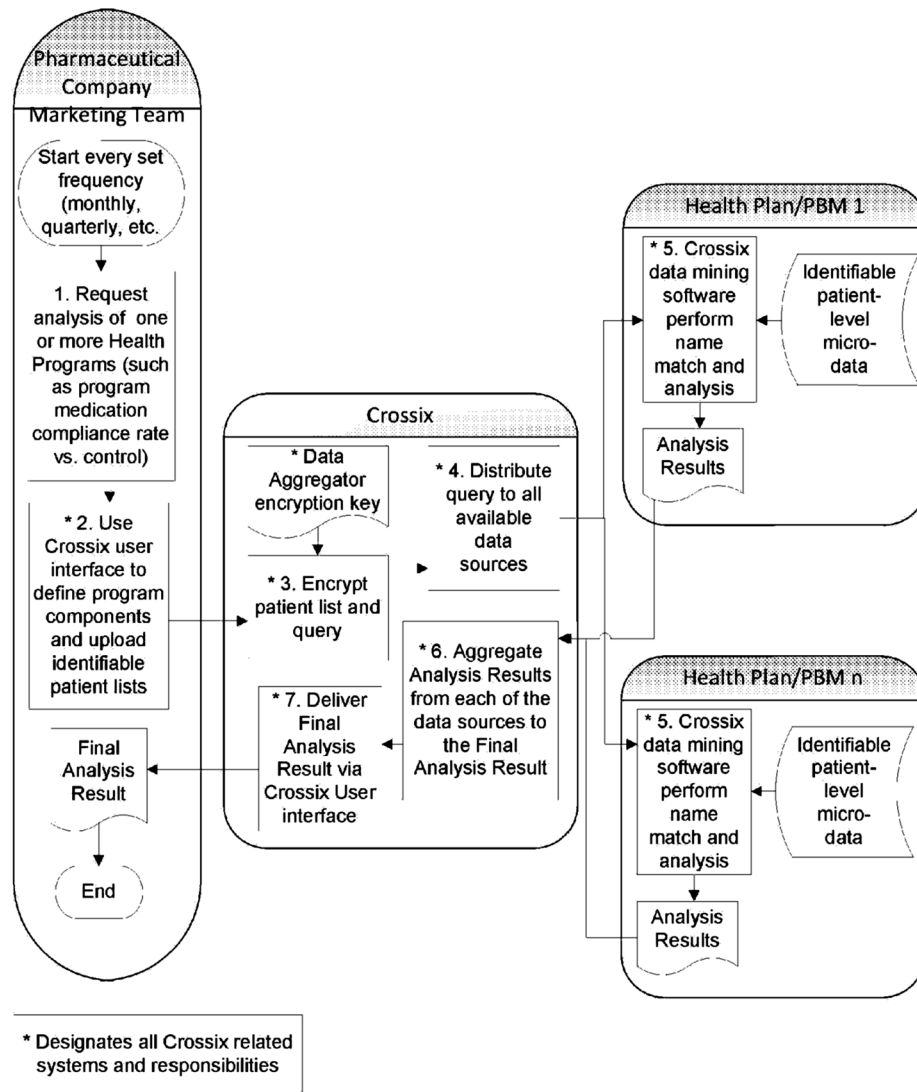


FIG. 4

Figure 4 is a diagram that “illustrate[s] detailed aspects” of Evenhaim’s preferred embodiment. Ex. 1005, 14:48–49. This protocol includes a query for group statistics on protected information of identified persons, at least one secure “source-entity” database of the protected information, and one secure data “aggregator” that receives the query and reports the group statistics. *Id.* at 7:32–63.

In the example illustrated in Figure 4, a pharmaceutical entity provides a formalized query seeking statistics from HMOs on a group of persons that are identified by name (or the like) in the query. Ex. 1005, 7:65–8:43, 9:6–10, Fig. 4 (steps 1 and 2). Using an encryption key, the aggregator encrypts the protected personal information of the query and then distributes the encrypted query to the source-entity databases. *Id.* at 8:47–9:18, Fig. 4 (steps 3 and 4). The source-entity “crunch[es] together” all data items responsive to the parameter list of the query (e.g., including the responsive protected personal information). *Id.* at 9:39–51, Fig. 4 (step 5). The source-entity then filters out (i.e., eliminates) from the crunched data items all portions that might allow guessing the identity of some data attributes. *Id.* at 9:50–63. A file of the crunched, remaining data items is then transmitted to the aggregator “according to well-known methods in the art.” *Id.* at 9:64–67.

Lastly, the aggregator extracts the received “query relevant data” of the source-entities, forms resulting “single temporary collections” of the extracted data, and “agglomerat[es] the extract [into] a condensed picture of all of the data.” Ex. 1005, 9:18–28, Fig. 4 (step 6) (internal quotations omitted). Finally, the agglomerate of extracted data is reported to the querying entity. *Id.* at 9:18–28, Fig. 4 (step 7).

Evenhaim also presents “[a] further class of embodiments” using common encryption keys to encrypt portions of the data for linking records:

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.

Ex. 1005, 12:7–16.

2. *Murphy (Ex. 1009)*

Murphy describes a server application for “data obfuscation” applicable to data base query tools for medical information. Ex. 1009, 553. Murphy discloses an algorithm that blocks queries returning fewer than three patients, thereby protecting patient identity. *Id.* at 555.

3. *Petitioner’s Contentions Concerning Reasons to Combine the Teachings of Evenhaim and Murphy*

Petitioner cites Evenhaim as relating to data privacy in a distributed system using a protocol that includes creating an encryption “key” token to link medical records to an individual without compromising the individual’s identity, e.g., by replacing PII with a unique encryption key, such as a one-way hash. Pet. 10 (citing Ex. 1005, 12:4–20, 12:36–47; Ex. 1003, Clark Decl. ¶ 40). Petitioner notes that Evenhaim describes a system in which a processor (data aggregator), data sources (e.g., healthcare facilities), and source-entity processors are interconnected via a network. *Id.* at 12 (citing Ex. 1005, 6:57–63; Ex. 1003, Clark Decl. ¶ 39). According to Petitioner, Evenhaim teaches (i) the data aggregator receives queries with a list of patient names and encrypts the names, i.e., creates an encrypted token for each individual, and (ii) the data sources/servers use similar corresponding encrypted tokens (a common encryption key) to de-identify and match patient records, allowing the data sources to return de-identified health information for patients on the list. *Id.* Petitioner further notes that in Evenhaim either processor, i.e., on the data aggregator side or on the data source side, can execute the steps of the protocol. *Id.* at 14 (citing Ex. 1005, 17:53–63). Petitioner emphasizes that an ordinarily skilled artisan would have understood Evenhaim’s token matching as teaching an efficient way to

query de-identified data to ensure compliance with HIPAA. *Id.* (citing Ex. 1005, 9:29–34, 12:4–13:20, 11:31–46; Ex. 1003, Clark Decl. ¶¶ 46–47).

Petitioner cites Murphy as describing a study to prevent the identification of individuals in a search of a medical database using an algorithm that blocks queries returning information from fewer than three patients, thereby preventing disclosure of the patient’s identity. Pet. 14–15 (citing Ex. 1009, 552–53, 555; Ex. 1003, Clark Decl. ¶ 66). Petitioner contends that a person of ordinary skill would have had reason to combine the teachings of Evenhaim and Murphy because Murphy describes how to use query responses that maintain patient privacy (a stated goal of Evenhaim) using volume to mask patient identity in order to comply with the statistical de-identification provisions of HIPAA. *Id.* at 15–16 (citing Ex. 1003, Clark Decl. ¶ 68; Ex. 1005, 14:7–13).

On the current record, we determine that Petitioner has demonstrated a person of ordinary skill would have had reason to combine the teachings of Evenhaim and Murphy, at least because both are explicitly related to systems that provide medically relevant information in response to a query in compliance with HIPAA requirements concerning data privacy and de-identification of individual patient data.

4. *Analysis of Representative Claim 7*

a) *Limitation 7.a*

Petitioner identifies as limitation [7.a] the recitation “[a] system comprising: a computing device comprising: a memory configured to store instructions; and a processor to execute the instructions to perform operations.” Petitioner cites Evenhaim as disclosing a server that sends the request for information (data aggregator) as well as a data server that responds to the request for information (data source, source entity or data

source entity) both of which connect with other machines using the Internet. Pet. 16 (citing Ex. 1005, 6:34–42). Petitioner notes that both the data aggregator and data source entity have processors for executing a protocol. *Id.* at 17 (citing Ex. 1005, 17:53–63; Ex. 1003, Clark Decl. ¶¶ 71–74). Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated Evenhaim would have disclosed or suggested this limitation to an ordinarily skilled artisan.

b) Limitation 7.b

Petitioner identifies as limitation [7.b] the recitation “receiving a request from a user device for information that characterizes a group composed of multiple individuals.” Pet. iv. Petitioner cites Evenhaim as disclosing information requests drawn to specific individuals or requests having predetermined attributes for a group, e.g., a group of patients having common treating physicians or health outcomes of patients in a clinical trial. *Id.* at 17–18 (citing e.g., Ex. 1005, 6:64–67, 8:4–13, 8:65–9:12, 15:3–14, 15:25–45; Ex. 1003, Clark Decl. ¶ 76). Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated Evenhaim would have disclosed this limitation to an ordinarily skilled artisan.

c) Limitation 7.c

Petitioner identifies as limitation [7.c] the recitation “from a set of de-identified data representing characteristics of the individuals pre-or post-encounter with a healthcare facility.” Pet. iv. Petitioner cites Evenhaim as disclosing its system can be used to request information that assesses the impact of health programs, such as the outcome of patients in a clinical trial. *Id.* at 18–19 (citing e.g., Ex. 1005, 7:12–26, 8:65–9:12, 15:3–14, 15:25–45; Ex. 1003, Clark Decl. ¶¶ 77–78). Petitioner contends that, because such data includes diagnosis, treatment, pharmacy, and clinical data, a person of

ordinary skill would have understood the information is about a group of individuals post-encounter with a healthcare facility. *Id.* (citing Ex. 1005, 15:3–20, Fig. 4A; Ex. 1003, Clark Decl. ¶ 79). Petitioner cites Evenhaim’s description of comparing health information from individuals who took part in a health program to that of a control group, noting that the control group may include individuals before or pre-encounter with a healthcare facility. *Id.* at 19 (Ex. 1003, Clark Decl. ¶ 79). Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated Evenhaim would have disclosed or suggested this limitation to an ordinarily skilled artisan.

d) Limitation 7.d

Petitioner identifies as limitation [7.d] the recitation “wherein the request contains identifying data for each member in the group of multiple individuals who have had an encounter with a healthcare facility.” Pet. iv. Petitioner cites Evenhaim as disclosing that the parameter list in a request may include individually identifying information, such as names, dates of birth, or the like. *Id.* at 20 (citing, e.g., Ex. 1005, 8:39–43, 8:18–22, 13:62–14:13; Ex. 1003, Clark Decl. ¶ 80).

Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated Evenhaim would have disclosed or suggested this limitation to an ordinarily skilled artisan.

e) Limitation 7.e

Petitioner identifies as limitation [7.e] the recitation “producing, by a hardware processor, a request token for each individual included in the group of individuals.” Pet. iv. Noting Evenhaim discloses that, after receiving an information request pertaining to a list of patients, the data aggregator applies an encryption key to encrypt those patients, Petitioner asserts that a person of ordinary skill would have appreciated that this

process creates tokens for each individual. *Id.* at 21 (citing Ex. 1005, Fig. 4, 12:4–13:20, 8:18–22; Ex. 1003, Clark Decl. ¶¶ 81–84). Arguing that token creation and matching have been well known since the 1980s, Petitioner asserts that an ordinarily skilled artisan would have understood that token creation and matching described in Evenhaim could be applied to the embodiment in Figure 4 such that the aggregator would create encrypted tokens from a list of patients received. *Id.* at 21–22 (citing Ex. 1005, 12:4–13:20; Ex. 1003, Clark Decl. ¶¶ 81–84). Petitioner further cites Evenhaim as explaining that token creation could be performed by the aggregator as well as the data sources. *Id.* at 22 (citing Ex. 1005, 12:24–34, 17:53–63; Ex. 1003, Clark Decl. ¶¶ 71–72).

Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated Evenhaim would have disclosed or suggested this limitation to an ordinarily skilled artisan.

f) Limitation 7.f

Petitioner identifies as limitation [7.f] the recitation “comparing the request tokens to tokens associated with the medical data to find matching tokens.” Pet. iv. Petitioner cites Figures 4 and 4A of Evenhaim as illustrating that tokens, in the form of unique encryption keys created from PII using a one-way hash, are sent from the aggregator to the data sources and argues that it is obvious the data sources match received tokens to corresponding tokens in a set of de-identified patient records. *Id.* at 22 (citing Ex. 1005, 12:4–47 (for the proposition that the encryption key is used on the data source side to de-identify the records), 17:27–40 (for the proposition that tokenization may occur before searching); Ex. 1003, Clark Decl. ¶¶ 84–86). Petitioner points out that Figure 4, box 4, shows a query sent to the data sources, which perform matching in box 5 and then return

the results to the aggregator in box 6. *Id.* According to Petitioner, an ordinarily skilled artisan applying the features in the embodiment of Figure 4 would have produced tokens created from the parameter list received by the data aggregator (box 3) using a common encryption key for the query, so that the tokens could be matched to corresponding tokens on the data source side with matching records being returned to the aggregator in box 6. *Id.* at 25–26 (citing Ex. 1005, 12:4–16, 12:27–33, 12:37–41; Ex. 1003, Clark Decl. ¶ 86). Petitioner further notes that this approach would both locate relevant records and ensure that multiple records from the same patient are matched together even after de-identification. *Id.* at 26 (citing Ex. 1005, 12:49–52).

Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated Evenhaim would have disclosed or suggested this limitation to an ordinarily skilled artisan.

g) Limitation 7.g

Petitioner identifies as limitation [7.g] the recitation “and to determine whether the group includes at least a minimum number of individuals to be included in a report in response to the request.” Pet. iv. Petitioner cites Evenhaim as explaining that, in order to protect privacy, a sufficient population is required to prevent a definitive conclusion about the personal data of any individual. *Id.* at 26–27 (citing Ex. 1005, 13:62–65, 8:13–48, 16:5–32; Ex. 1003, Clark Decl. ¶¶ 87–88). Petitioner further cites Murphy as disclosing that, in complying with HIPAA, an algorithm blocks queries from returning information about fewer than three patients to prevent the user from associating a patient with his/her record. *Id.* (citing Ex. 1009, 555; Ex. 1003, Clark Decl. ¶ 89).

Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated Evenhaim and Murphy would have disclosed or suggested this limitation to an ordinarily skilled artisan.

h) Limitation 7.h

Petitioner identifies as limitation [7.h] the recitation “wherein the minimum number of individuals are selected according to at least a privacy-preserving rule that disallows same individuals to be included within a defined period of time.” Pet. iv. Petitioner cites both Evenhaim and Murphy as suggesting the requirement for a minimum number of individuals for privacy purposes. *Id.* at 27. Petitioner further argues that an ordinarily skilled artisan would apply Murphy’s concept of auditing queries in a history table to check the date/time and the number of individuals returned by queries to disallow repeated use of the same individual in a query. *Id.* (citing Ex. 1009, 554; Ex. 1003, Clark Decl. ¶ 91). Petitioner notes Murphy’s explanation that checking the number of individuals returned in the query against the number of individuals returned in the previous query in a predetermined time period helps prevent reverse engineering the identity of individuals. *Id.* at 27–28 (citing Ex. 1009, 554; Ex. 1003, Clark Decl. ¶ 91).

Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated the combined teachings of Evenhaim and Murphy would have disclosed or suggested this limitation to an ordinarily skilled artisan.

i) Limitation 7.i

Petitioner identifies as limitation [7.i] the recitation “producing the requested information that characterizes the group.” Pet. iv. Petitioner cites Evenhaim as disclosing that the health care information produced reports

include characteristics (medical information) of a group and may include the de-identified patient records themselves. *Id.* at 28 (citing, e.g., Ex. 1005, 10:6–11, 15:3–14, Fig. 4; Ex. 1003, Clark Decl. ¶ 92).

Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated Evenhaim would have disclosed this limitation to an ordinarily skilled artisan.

j) Limitation 7.j

Petitioner identifies as limitation [7.j] the recitation “an identity of the individuals being unattainable from the produced information.” Pet. iv. Petitioner notes that Evenhaim describes the produced healthcare information does not include personally identifiable information because the data is de-identified. *Id.* at 28 (citing, e.g., Ex. 1005, 9:13–18; Ex. 1003, Clark Decl. ¶ 93).

Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated Evenhaim would have disclosed or suggested this limitation to an ordinarily skilled artisan.

k) Limitations 7.k and 7.l

Petitioner identifies as limitation [7.k] the recitation “and providing the produced medical information to report the characteristics of the group of individuals.” Pet. iv. Petitioner identifies as limitation [7.l] the recitation “absent authorization from the individuals in the group of individuals identified in the request containing identifying data.” *Id.* As to limitation [7.k], Petitioner cites Evenhaim as disclosing the various types of health information characterizing the group are provided including the de-identified medical records. *Id.* at 28 (citing, e.g., Ex. 1005, Fig. 5, 7:12–26, 8:65–9:12, 15:3–14, 15:25–45; Ex. 1003, Clark Decl. ¶ 94). As to limitation [7.l], Petitioner cites Evenhaim’s goal of producing de-identified healthcare

information that can be released to third parties without the consent of individuals in the group compliance with HIPAA. *Id.* at 29 (citing, e.g., Ex. 1005, 3:17–31, 4:34–48, 5:46–6:10, 8:18–22, 14:7–13, 15:15–24, 14:59–67, 3:26–31; Ex. 1003, Clark Decl. ¶ 95).

Based on the disclosure cited by Petitioner, we determine that Petitioner has demonstrated Evenhaim would have disclosed or suggested these limitations to an ordinarily skilled artisan.

l) Conclusion As To Representative Claim 7

In consideration of the above, we are persuaded for purposes of this Decision that Petitioner has cited sufficient evidence to demonstrate a person of ordinary skill would have been motivated to combine the teachings of Evenhaim and Murphy and their combined teachings would have disclosed or suggested all the limitations of claim 7 to a person of ordinary skill in the art.

5. Independent Claims 1 and 14

Independent claim 1 is drawn to a method and recites steps that correspond to the operations recited in claim 7. Independent claim 14 is drawn to a computer readable storage medium storing instructions executable by a processing device to perform operations that correspond to those in claim 7. For the same reasons as those addressed in our discussion of claim 7, we determine that Petitioner has demonstrated that Evenhaim and Murphy teach the limitations of independent claims 1 and 14.

6. Dependent Claims 2–6, 8–13, and 15–20

Claims 2–6 depend from claim 1, claims 8–13 depend from claim 7, and claims 15–20 depend from claim 14. Claims 2, 8, and 15 recite that the provided information is medical information in conformity with HIPAA. Petitioner cites Evenhaim as being directed to such information. *See* Pet. 29.

Claims 3, 9, and 16 recite that the request for information that characterizes a group of individuals includes PII associated with those individuals. Petitioner cites Evenhaim's description of a user request including a parameter list that may includes names, and other PII information. *See* Pet. 29.

Claims 4, 10, and 17 recite that the data identifying each individual is encrypted. Petitioner cites Evenhaim as disclosing this feature. *See* Pet. 29–30. Claims 5, 11, and 18 recite that the tokens associated with the data and the request are similarly encrypted. Petitioner cites Evenhaim's use of a common encryption key to ensure that records can be matched as disclosing this feature. *See id.* at 30.

Claims 12 and 20 recite that producing the requested information includes determining if the group includes a minimum number of individuals. Petitioner cites its discussion of limitations [7.g] and [7.h] as demonstrating that Evenhaim and Murphy in combination discloses this feature. *See* Pet. 31.

Claims 6, 13, and 19 recite that the data represents medical-related information associated with individuals of the group. Petitioner cites Evenhaim as disclosing the medically related data includes patient-level microdata. *See* Pet. 31 (citing Ex. 1005, Figs. 1–2, 5; 10:46–54, 11:14–29, 12:36–47).

For purposes of this Decision, we determine that Petitioner has cited sufficient evidence to demonstrate that a person of ordinary skill would have been motivated to combine the teachings of Evenhaim and Murphy and that their combined teachings would have disclosed or suggested all the limitations of claims 2–6, 8–13, and 15–20 to a person of ordinary skill in the art.

C. Petitioner’s Contentions That Claims 1–20 Are Unpatentable as Obvious over Evenhaim and Settimi

1. *Settimi (Ex. 1006)*

Settimi is titled “Systems and Methods for Identification of Clinical Study Candidates.” Ex. 1006, code (54). Settimi relates to the searching and analysis of electronic medical record data to identify clinical study participants “based on electronic medical record data.” *Id.* ¶ 4. Settimi describes data warehouses that “aggregate, clean, stage, report and analyze patient information . . . extracted from [databases of] patient care provider (PCP) sites.” *Id.* ¶ 9. Settimi explains that the protected personal information must be removed (per HIPAA) from patient information sent by PCP sites to a data warehouse, and that “[r]emoving [such] data . . . can make it impossible to group and analyze all medical reports relating to a particular patient.” *Id.* ¶¶ 9–10.

Settimi further describe “a secure process for sending de-identified patient information from an ambulatory patient care provider (PCP) site to a data warehouse system where the patient data may be analyzed and compared with a wider range of patient data.” Ex. 1006 ¶ 27.

This process is illustrated Figure 3 of Settimi following.

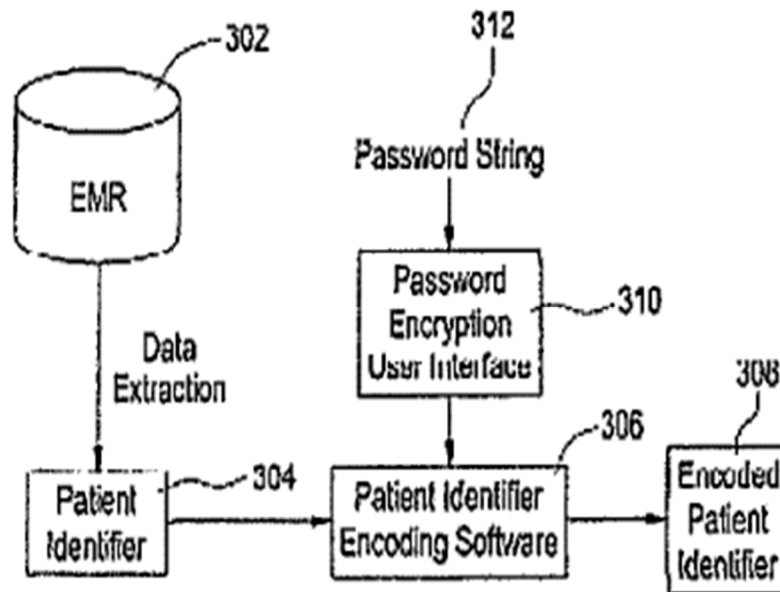


Figure 3 is a block diagram illustrating a process for de-identifying patient data during data extraction for transmission to a data warehouse. Ex. 1006 ¶ 38. Patient data extracted from an electronic medical record (EMR) database 302 and personal identifying information is “removed or transformed in order to create de-identified data.” *Id.* ¶¶ 38–39. In the given example, de-identifying includes transforming each patient’s patient identifier (PID) 304 to a unique encoded patient identifier (EPID) 308 based on the PID 304 and a password entered by the PCP. *Id.* ¶ 41. A patient’s de-identified data thereby includes “an EPID 308 that may be useful in creating longitudinal reports that analyze more than one record for a particular patient.” *Id.* ¶ 43. Accordingly, in the data warehouse receiving the de-identified patient data, “[d]e-identified individuals may be tracked longitudinally and queried as members of anonymous population cohorts, based on clinical selection criteria,” and denoted in a “cohort report [as] a list of EPIDs 308” and respective data. *Id.* ¶ 42.

2. *Petitioner's Contentions Concerning Motivation to Combine the Teachings of Evenhaim, Settimi, and Murphy*

Petitioner notes that, where Evenhaim sends healthcare data queries to various healthcare organizations, Settimi consolidates the information from various providers in a central repository for queries. Pet 40–41 (citing Ex. 1005, 15:15–24, 16:5–21, Fig 4; Ex. 1006, Figs. 1–2, ¶ 27; Ex. 1003, Clark Decl. ¶ 137). According to Petitioner, Settimi's repository eliminates the need for conducting searches across different entities and uses a “common vocabulary” that makes searching easier and more reliable. *Id.* (citing Ex. 1006 ¶¶ 9, 60–62; Ex. 1003, Clark Decl. ¶ 136). Petitioner further cites Settimi as disclosing generating encoded patient identifiers (EPIDs) for individuals, i.e., encrypted tokens, based, e.g., on a patient's name or Social Security number, and querying the repository to obtain records without revealing the patient's identity. *Id.* at 40 (citing Ex. 1006 ¶ 37). According to Petitioner, a person of ordinary skill would have had reason to combine the teachings of Evenhaim and Settimi to simplify querying with a single query to a single repository using a standardized search vocabulary, while still allowing for searches for specific patients. *Id.* at 41–42 (citing Ex. 1006 ¶ 60; Ex. 1003, Clark Decl. ¶¶ 135–137). For purposes of this Decision, we determine that Petitioner has demonstrated a person of ordinary skill would have had reason to apply the teachings of Evenhaim to a central repository, as disclosed in Settimi.

We also determine that Petitioner has demonstrated that an ordinarily skilled artisan would have had reason to further combine the teachings of Evenhaim and Settimi with those of Murphy, in a manner similar to that discussed above, to ensure the result of the query would not be sufficiently small such that an individual could be identified. *Id.* at 42.

3. *Analysis of Representative Claim 7*

As to the subject matter identified by Petitioner as limitations [7.a–7.1], Petitioner cites the teachings of Evenhaim as discussed previously. Pet. 43. Petitioner further discusses Settimi’s disclosure concerning several specific limitations.

As to limitation [7.c], Petitioner also cites Settimi as disclosing embodiments in which de-identified patient information is securely sent from a patient care provider (PCP) site to a data warehouse for analysis and comparison with a wider range of patient data. Pet. 43 (citing Ex. 1006 ¶ 27). Petitioner further notes Settimi’s disclosure that information obtained through the data warehouse pertaining to individual patients is transmitted back to the original PCP site via a cohort report and argues that an ordinarily skilled artisan would understand such patient data is usually recorded after a patient’s medical visit with the doctor or other healthcare provider. *Id.* (citing Ex. 1003, Clark Decl. ¶¶ 140–141).

As to limitation [7.d], Petitioner notes that the requests in both Evenhaim and Settimi are for healthcare information that characterizes a group of individuals after an encounter with a healthcare facility. Pet. 43–44. As to limitation [7.e], Petitioner contends that an ordinarily skilled artisan would apply Settimi’s concept of a central warehouse to Evenhaim, noting that Settimi’s data warehouse would replace the PBMs (PBM 1–n) in Evenhaim’s Figure 4 embodiment. Petitioner further asserts that, because Settimi’s central warehouse contains only de-identifies records in which the PII has been replaced with an encrypted token, an ordinarily skilled artisan would have understood that an encrypted patient list sent in Evenhaim’s steps 3–4 would use encryption that allows for finding matching records in the central warehouse. *Id.* Petitioner further notes that Settimi also explains

tokens are used to identify all the records for particular patients. *Id.* at 45–46 (citing Ex. 1006 ¶¶ 35, 37).

As for comparing request tokens to tokens associated with medical data to find matching tokens, as recited in limitation [7.f], Petitioner argues that an ordinarily skilled artisan would have understood that to make the query called for in Evenhaim in a database such as Settimi’s “a matching token would be produced for each individual on the list to identify the relevant records, because the central warehouse contains only de-identified data.” Pet. 46–47 (citing Ex. 1003, Clark Decl. ¶ 150). Observing that no names or other PII could be used in the query in Settimi because the centralized warehouse has no such information, Petitioner states that a person of ordinary skill would have understood that searching for particular patients as described in Evenhaim would be accomplished in Settimi using the encrypted tokens, as that is how records are identified in Settimi’s central warehouse. *Id.* at 47 (citing Ex. 1003, Clark Decl. ¶ 150; Ex. 1006 ¶ 37). As to limitation [7.j], Petitioner notes that cohort reports produced by Settimi connect all records relating to a single patient in the data warehouse using a unique identifier associated with each patient record that does not provide personal direct identifying information. *Id.* at 49 (citing Ex. 1006 ¶¶ 27, 30, 35–37, 39–42; Ex. 1003, Clark Decl. ¶ 156).

4. *Conclusion as to Representative Claim 7*

Having considered the arguments and evidence of record, we are persuaded for purposes of this Decision that Petitioner has cited sufficient evidence to demonstrate that a person of ordinary skill would have been motivated to combine the teachings of Evenhaim, Settimi, and Murphy and their combined teachings would have disclosed or suggested all the limitations of claim 7 to a person of ordinary skill in the art.

5. *Independent Claims 1 and 14*

Independent claim 1 is drawn to a method and recites steps that correspond to the operations recited in claim 7. Independent claim 14 is drawn to a computer readable storage medium storing instructions executable by a processing device to perform operations that correspond to those in claim 7. For the same reasons as those addressed in our above discussion of claim 7, we determine that Petitioner has demonstrated that the combination of Evenhaim, Settini, and Murphy teaches the limitations of independent claims 1 and 14.

6. *Dependent Claims 2–6, 8–13, and 15–20*

Claims 2–6 depend from claim 1, claims 8–13 depend from claim 7, and claims 15–20 depend from claim 14. Petitioner contends that claims 2–6, 8–13, and 15–20 are unpatentable for essentially the same reasons as those Petitioner articulated in its arguments concerning Evenhaim and Murphy. Pet. 52–56.

For purposes of this Decision, we determine that Petitioner has cited sufficient evidence to demonstrate that a person of ordinary skill would have been motivated to combine the teachings of Evenhaim, Settini, and Murphy and their combined teachings would have disclosed or suggested all the limitations of claims 2–6, 8–13, and 15–20 to a person of ordinary skill in the art.

D. Petitioner’s Contentions That Claims 1–20 Are Unpatentable as Obvious over Dick, Landi, and Murphy

1. *Dick (Ex. 1007)*

Dick is titled “Method and Apparatus for Requesting and Retrieving De-Identified Medical Information.” Ex. 1007, code (54). Dick “relates generally to electronic access of medical information” such as “medication,

pharmaceutical, and clinical information.” *Id.* ¶ 2. This access is summarized as searching for medical information of a person (or persons) via a request to a medical information repository and receiving a response that includes respective, de-identified medical information. *Id.* ¶¶ 11–12.

In an example, the interacting entities are “requesting and viewing clients” (RVCs), a central server, and medical information repositories. Ex. 1007 ¶¶ 20, 27–28. A request for medical information sent by an RVC to the central server 245 includes a person or group of persons identified by name(s) (or the like), that constitutes the target of the search. *Id.* ¶¶ 24, 27. The central server transmits a respective query to the medical information repository. *Id.* ¶ 28. The medical information repository de-identifies the respective medical information before releasing the information (i.e., de-identifies the query response). *Id.* ¶ 45.

2. *Landi (Ex. 1008)*

Landi is titled “Systems and Methods for Encryption-Based De-Identification of Protected Health Information.” Ex. 1008, code (54). Landi “relates, in general, to protecting patient privacy when healthcare information is shared between various healthcare entities and, in particular, to . . . secured key encryption for de-identifying patient data to ensure patient privacy.” *Id.* at 1:14–19. Landi describes conventional methods for de-identifying patient data that involve either striping out identifying information or substituting other information, (e.g., replacing an actual name with a with a “string ‘name.’”) *Id.* at 2:19–24.

Landi discloses an “exemplary embodiment” summarized as “obtaining a data record of an individual which includes individual identifying information, removing the individual identifying information in the data record to generate a de-identified data record, generating an

encrypted [respective] ID . . . , and storing the encrypted ID with or in the de-identified data record.” Ex. 1008, 2:41–49.

The patient data processing systems release de-identified patient data records to the central patient data processing system for purposes of research, health care monitoring, etc. Ex. 1008, 4:11–28. The patient data processing systems use the same secure public encryption protocol to encrypt patient identifying information and, as part thereof, associate within the information of each included patient (e.g., insert within) an “Encrypted ID” constituting a “reproducible encrypted version of [the] patient identifying information” and “uniquely identify[ing] the patient.” *Id.* at 4:65–5:15, 5:32–36.

3. *Petitioner’s Contentions Concerning Motivation to Combine the Teachings of Dick and Landi*

Petitioner cites Dick as describing “a system for requesting and retrieving de-identified medical information for a group of individuals in which a client device requests information that characterizes a group and that request is sent to an information repository that returns de-identified health information in response.” Pet. 57 (citing Ex. 1007, code (57), ¶¶ 20–24, 45–46, claim 23; Ex. 1003, Clark Decl. ¶ 54). Petitioner acknowledges that, although Dick states de-identification can occur at any number of locations, such as the medical repository or the originating source of the information, Dick does not describe any specific de-identification methods. *Id.* at 57–58 (citing Ex. 1003, Clark Decl. ¶¶ 55, 196–199). Recognizing this absence of disclosure in Dick, Petitioner argues that a person of ordinary skill would have looked elsewhere for information on implementing de-identification as called for in Dick. *Id.* at 58 (citing Ex. 1003, Clark Decl. ¶ 200). Petitioner notes that both Dick and Landi concern compliance with

HIPAA and are directed to using central repositories to provide a collection of medical records for searching; Petitioner contends that an ordinarily skilled artisan would have looked to Landi’s description of Encryption IDs created using a common public key to facilitate a token matching system used to locate medical records, such as those in Dick. *Id.* at 58–62 (citing Ex. 1003, Clark Decl. ¶¶ 58, 199). For purposes of this Decision, we determine that Petitioner has demonstrated that an ordinarily skilled artisan would have had reasons to combine the teachings of Dick and Landi, because Landi teaches a method to search medical databases and return the de-identified results discussed in Dick. We further agree that an ordinarily skilled artisan would have had reason to combine Dick and Landi with Murphy because Murphy describes how to use query responses that maintain patient privacy (a goal of Dick and Landi) using volume to mask patient identity in compliance with HIPAA. *Id.* at 61 (citing Ex. 1003, Clark Decl. ¶ 204).

4. *Analysis of Representative Claim 7*

Beginning with claim limitations [7.a] and [7.b], Petitioner cites Dick as disclosing a system in which Requester’s Server 230 receives a request from a “requesting and viewing client” to obtain from a Medical Information Repository (central server 245) medical records for a “subject” that may be “human individual or group of humans.” Pet. 63 (citing Ex. 1007, Figs. 1–3, ¶¶ 20–21, 24, 44–46; Ex. 1003 ¶ 209). Petitioner cites Landi as disclosing central database/system 30 containing only de-identified records in which PII has been replaced with tokens (Encrypted IDs) for each individual that has patient records. *Id.* at 63–64 (citing Ex. 1008, 4:40–46; Ex. 1003, Clark Decl. ¶¶ 210–211). Petitioner further notes Landi’s Encrypted IDs are created using freely distributable public keys that allow various entities to

replicate the Encrypted IDs when dealing with the same patient. *Id.* (citing Ex. 1008, 8:39–55, 4:65–5:19, 5:32–44, 5:57–61; Ex. 1003, Clark Decl. ¶¶ 210–212).

Claim limitation 7[c] recites that the request is for information from a set of de-identified data representing the characteristics of individuals pre- or post-encounter with a healthcare facility. Pet. 65. Petitioner cites Dick as disclosing medical information 100 encompasses information relating to physical and mental health diagnoses and remedies, such as physician-patient records, clinical information records (e.g., laboratory testing), and prescription drug records. *Id.* at 65–66. Petitioner notes that Dick discloses information can be de-identified at any of a number of points including the originating source of the information, such as the PMP or the clinic from which the medical information is being collected. *Id.* (citing Ex. 1007 ¶¶ 18, 46; Ex. 1003, Clark Decl. ¶¶ 215–216).

As to limitation [7.d], which recites that the request contains identifying data for each member having an encounter with a healthcare facility, Petitioner cites Dick as disclosing (i) receiving a request for medical information including the identification of the subject and (ii) searching the medical information repository medical information regarding the group of preselected individuals. Pet. 66 (citing Ex. 1007 ¶¶ 19–22, 24, claim 23; Ex. 1003, Clark Decl. ¶ 217). Petitioner cites Landi as describing its ability to monitor patients in a clinical trial, while still complying with HIPAA. *Id.* (citing Ex. 1008, 9:43–10:15). According to Petitioner, an ordinarily skilled artisan would have appreciated that when patients are queried under this scenario, tokens (Encrypted IDs) are created using PII for each patient in the trial. *Id.* at 66–67 (citing Ex. 1008, 9:52–56).

As to limitation [7.e], which recites that the hardware produces a request token for each individual, Petitioner argues that a person of ordinary skill would have been motivated to produce a token for each individual in Dick's group of individuals in a query because (i) Dick's system includes a remote database for medical records for the group of individuals, (ii) Landi's central database of de-identified patient records identifies the records through Encrypted IDs, and (iii) the public keys for creating such tokens are freely distributed in compliance with HIPAA in order to allow for recognition of corresponding records. Pet. 64, 67 (citing Ex. 1007, Fig. 2, 3, ¶¶ 8, 11, 24; Ex. 1008, 7:3–38, 8:39–55). Accordingly, because the public keys create matching tokens in the query and in the de-identified records, the tokens (Encrypted IDs) stored in Landi's central processing system 30 correspond to the same tokens produced by Dick's server in response to the user request. *Id.* at 67. Petitioner argues that this correspondence facilitates matching request tokens to medical data tokens, as recited in limitation [7.f]. *Id.* at 67–68.

As to claim limitation [7.g], which recites that the group includes at least a minimum number of individuals to be included in a report, Petitioner acknowledges that Dick does not explicitly disclose this feature. Pet. 69. Petitioner cites Murphy as disclosing an algorithm that blocks queries that return fewer than three patients to prevent the user from associating the patient with particular record in order to comply with HIPAA. *Id.*

Claim limitation [7.h] recites that the minimum number of individuals are selected according to a privacy-preserving rule that disallows the same individuals from being included within a defined period of time. Pet. 69–70. Petitioner cites Murphy as disclosing the benefits of checking whether a number of individuals returned in the query return the exact number of

individuals as that of the previous query within a predetermined time and preventing further queries. *Id.* (citing Ex. 1009, 554, discussing circumstances where the user is prevented from performing further queries “when a certain number of queries return the exact same number of patients”).

Claim limitations [7.i]–[7.k] recite producing the requested information that characterizes the group in the manner in which the identity of the individuals is unattainable and providing the medical information to report the characteristics of the group of individuals absent authorization. Pet. 70–71. Petitioner cites Dick as explaining that the medical information concerns the characteristics of a group of individuals and that the information is produced without individuals in the group authorizing its production. *Id.* Petitioner cites Landi as describing Encrypted IDs that prevent the identification of individuals as called for in Dick. *Id.* at 70.

5. *Conclusion as to Representative Claim 7*

Having considered the arguments and evidence of record, we are persuaded for purposes of this Decision, that Petitioner has cited sufficient evidence to demonstrate that a person of ordinary skill would have had reason to combine the teachings of Dick, Landi, and Murphy and their combined teachings would have disclosed or suggested all the limitations of claim 7 to a person of ordinary skill in the art.

6. *Independent Claims 1 and 14*

Independent claim 1 is drawn to a method and recites steps that correspond to the operations recited in claim 7. Independent claim 14 is drawn to a computer readable storage medium storing instructions executable by a processing device to perform operations that correspond to those in claim 7. For the same reasons as those addressed in our discussion

of claim 7, we determine that Petitioner has demonstrated that the combination of Dick, Landi, and Murphy teach the limitations of independent claims 1 and 14.

7. *Dependent Claims 2–6, 8–13, and 15–20*

Claims 2–6 depend from claim 1, claims 8–13 depend from claim 7, and claims 15–20 depend from claim 14. Claims 2, 8, and 15 recite that the provided information is medical information in conformity with HIPAA. Petitioner cites Dick as disclosing producing de-identified medical identification. Pet. 71.

Claims 3, 9, and 16 recite that the request for information that characterizes a group of individuals includes PII associated with those individuals. Petitioner cites Dick’s description of a request for healthcare information including the identification of a subject, which is PII. Pet. 71. Noting that Landi discusses its usefulness for monitoring patients in a clinical trial, Petitioner cites Landi as disclosing the request for healthcare information includes PII associated with members of a group. *Id.* at 71–72.

Claims 4, 10, and 17 recite that the data identifying each individual is encrypted. Petitioner cites Landi’s Encrypted IDs as disclosing this limitation. Pet. 72. Claims 5, 11 and 18 recite that the tokens associated with the data and the request are similarly encrypted. Petitioner cites Landi’s description that various entities create Encrypted IDs (tokens) using the same public keys as teaching this limitation. *Id.*

Claims 12 and 20 recite that producing the requested information includes determining if the group includes a minimum number of individuals. Petitioner cites its discussion of limitation [7.g] demonstrating that Dick, Landy and Murphy in combination disclose this feature. Pet. 72.

Claims 6, 13, and 19 recite that the data represents medical-related information associated with individual of the group. Petitioner cites Dick as disclosing a user's request is for medically related information that characterizes a group of individuals. Pet. 72–73. Petitioner also cites Landi's disclosure that healthcare data represents medical information associated with individuals in a group of individuals participating in a clinical trial. *Id.* at 73.

For purposes of this Decision, we determine that Petitioner has cited sufficient evidence to demonstrate that a person of ordinary skill would have been motivated to combine the teachings of Dick and Landi and their combined teachings would have disclosed or suggested all the limitations of claims 2–6, 8–13, and 15–20 to a person of ordinary skill in the art.

X. CONCLUSION

For the reasons discussed above, we are persuaded that Petitioner has demonstrated a reasonable likelihood that it will succeed on each of its challenges to patentability.

XI. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a) an *inter partes* review of claims 1–20 in the '651 patent is hereby instituted, commencing on the entry date of this Order, and 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;

FURTHER ORDERED that the trial is authorized on all grounds set forth in the Petition; and

IPR2024-00307

Patent 9.965,651 B1

FURTHER ORDERED that the trial will be conducted in accordance with a corresponding separately issued Scheduling Order.

IPR2024-00307
Patent 9.965,651 B1

FOR PETITIONER:

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

FOR PATENT OWNER:

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