

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

DATAVANT, INC.,  
Petitioner,

v.

VIGILYTICS LLC,  
Patent Owner.

---

IPR2024-00311  
Patent 10,109,375 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 1–22 (the “challenged claims”) of U.S. Patent No. 10,109,375 B1 (Ex. 1001, “the ’375 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 (2012). 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 (2018).

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

Petitioner and Patent Owner state that the ’375 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”). Pet. 1; Paper 3, 1.

#### IV. THE '375 PATENT

The '375 patent is titled “De-Identifying Medical History Information for Medical Underwriting.” Ex. 1001, code (54). The patent “relates to processing and transmitting personal data, the dissemination of which is restricted by federal law.” *Id.* at 1:16–18. Specifically, the patent relates to “de-identifying medical history information.” *Id.* at 1:42–43.

The patent discloses a “computer-implemented method” for “producing information that characterizes a group of individuals from a set of private data representing characteristics of the individuals.” Ex. 1001, 1:44–47. The identity of the individuals is unattainable from the produced information. *Id.* at 1:47–48. The method also includes providing the produced information to report the characteristics of the group. *Id.* at 1:49–50.

This operation is illustrated in Figure 3 of the '375 patent, reproduced below.

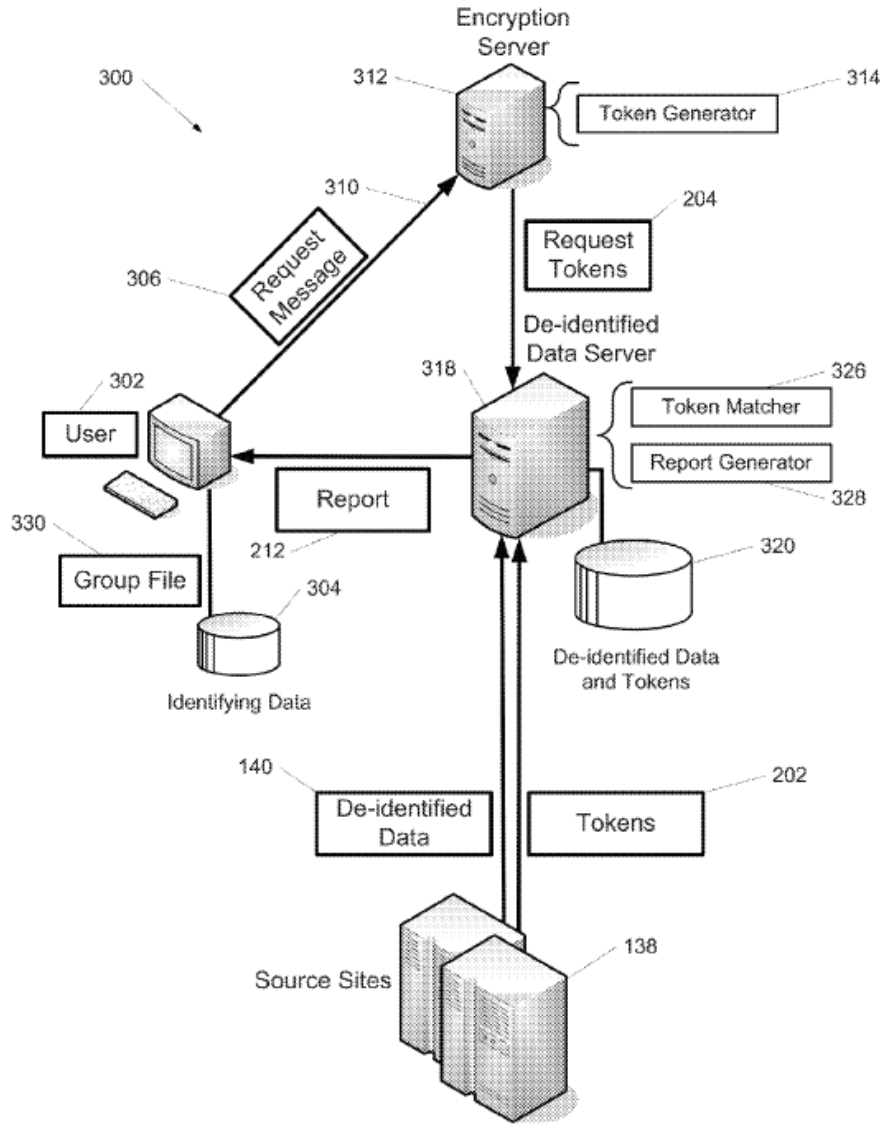


Figure 3 “illustrates an exemplary system incorporating an encryption server and a de-identified data server to enable a user who is not permitted to obtain the private data of a group of people to instead obtain a report that characterizes the group as a whole.” Ex. 1001, 3:5–9. In operation, request message 306 is sent over communications network 310 (e.g., the Internet) to encryption server 312. *Id.* at 5:33–35. 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 5:35–37.

The encryption server creates each token by applying token generator 314 that encrypts the personally identifiable information of each group member. Ex. 1001, 5:38–40. 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 5:42–45.

Encryption server 312 provides request tokens 204 to de-identified data server 318. Ex. 1001, 5:46–47. 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 5:47–51. 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 5:51–55.

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, 6:4–7. All available data for matched tokens, the requested de-identified data 208, is retrieved for use in report generator 328. *Id.* at 6:7–9.

## V. ILLUSTRATIVE CLAIMS

Claims 1, 7, and 14 are independent. Petitioner cites system claim 7 as illustrative of the subject matter claimed in the '375 patent. Independent claim 7 is reproduced below using the claim limitation designations in the Petition:

- [7.a] A system comprising: a data server device:
- [7.b] for producing healthcare information that characterizes a group of a number of individuals identified in a request

for the healthcare information that characterizes the group

- [7.c] wherein the request for healthcare information is sent to an encryption server that is configured to determine if the number of individuals in the request is at least a defined minimum number of individuals,
- [7.d] wherein a unique request token is produced for each individual included in the group
- [7.e] the data server is configured to compare the request tokens to tokens associated with healthcare data that includes de-identified information to find matching tokens,
- [7.f] the produced healthcare information is absent personally identifiable information and
- [7.g] is based on a minimum number of matched tokens,
- [7.h] the data server is also configured to provide the produced healthcare information to report the characteristics of the group
- [7.i] absent authorization from the individuals in the group.

*See* Pet. iv. Independent claim 1 is a method claim that recites steps generally corresponding to the operations carried out by the system recited in claim 7. *See* Ex. 1001, 10:31–54. 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 11:44–12:20.

## VI. ASSERTED GROUNDS

Petitioner asserts that claims 1–22 are unpatentable on the following grounds:

| Claim(s) Challenged | 35 U.S.C. §      | Reference(s)/Basis                            |
|---------------------|------------------|-----------------------------------------------|
| 1–22                | 103 <sup>1</sup> | Evenhaim, <sup>2</sup> Murphy, <sup>3</sup>   |
| 1–22                | 103              | Evenhaim, Settimi, <sup>4</sup> Murphy        |
| 1–22                | 103              | Dick, <sup>5</sup> Landi, <sup>6</sup> Murphy |

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

The level of ordinary skill in the art usually is evidenced by the references themselves. See *Okajima v. Bourdeau*, 261 F.3d 1350, 1355

---

<sup>1</sup> The Leahy-Smith America Invents Act (“AIA”) included revisions to 35 U.S.C. §§ 102 and 103 that became effective on March 16, 2013. The ’375 patent issued from a continuation application filed on June 5, 2015 (Ex. 1001, code (22)) and claims priority under 35 U.S.C. § 120 to an application filed on June 30, 2010. *Id.* at code (63), 1:7–10. We apply the pre-AIA version of the statutory basis for unpatentability.

<sup>2</sup> U.S. Pat. No. 7,823,207 (Ex. 1005)

<sup>3</sup> 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)

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

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

<sup>6</sup> U.S. Pat. No. 7,519,591 (Ex. 1008)

(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 ’375 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 construction 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                                   |
| Encryption server   | A server that produces tokens in response to a request.                                                                                                         |
| 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. 8.

Petitioner expressly “adopts these constructions for this proceeding without waiving its right to pursue alternative constructions in any future litigation.” Pet. 8. 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).

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*, 550 U.S. at 418–21).

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 1–22 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.

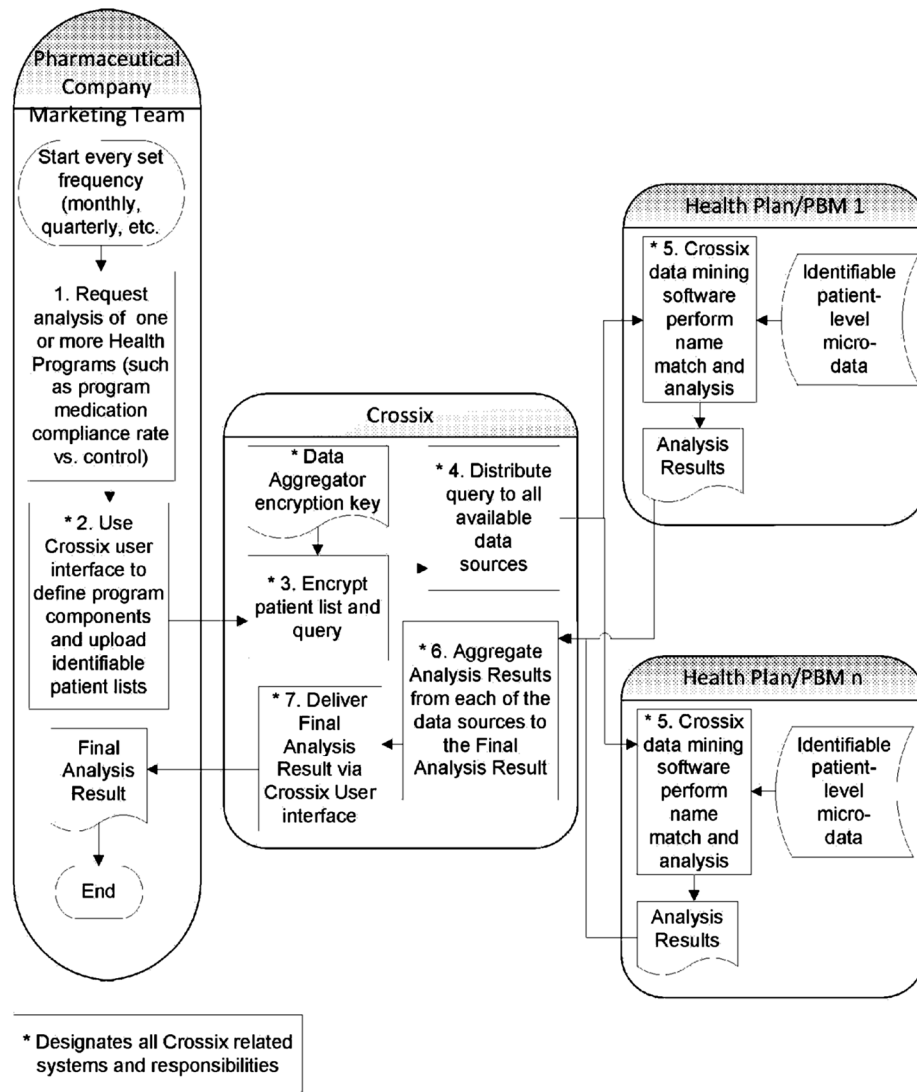


FIG. 4

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. 10–11 (citing Ex. 1005, 12:4–20, 12:36–47, 16:46–58, 17:27–41; Ex. 1003, Clark Decl. ¶¶ 39–40). According to Petitioner, Evenhaim’s encryption key is a token because it is an identifier associated with an individual that does not reveal the identity of the individual. *Id.* (citing Ex. 1003, Clark Decl. ¶ 40).

Petitioner notes that Evenhaim describes a system in which an encryption server (data aggregator), and at least one data server (data sources or source-entity processors) is interconnected via a network. Pet. 12 (citing Ex. 1005, 6:57–63; Ex. 1003, Clark Decl. ¶ 39). According to Petitioner, Evenhaim teaches (i) the data aggregator/server accepts a query, e.g., a list of patient names and encrypts the names, and 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.* at 12–13 (citing Ex. 1003, Clark Decl. ¶¶ 41, 44–46; Ex. 1005, Fig. 4, 12:4–13:20). Petitioner further

notes that “[a]t the very least” Evenhaim’s token matching would have been obvious to a person of ordinary skill, “given that token matching was well known in the field.” *Id.* at 14 (citing Ex. 1003, Clark Decl. ¶¶ 39–42).

Petitioner further argues that in Evenhaim the various servers “use a common encryption key” and can execute the steps of the protocol to match patients to their medical records, even though the patient names are not known on the data server. *Id.* (citing Ex. 1005, Fig. 4, 12:4–13:20; Ex. 1003, Clark Decl. ¶ 46). 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 (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 data server device.” Pet. iv. Petitioner cites Evenhaim as disclosing a data server (called a “data source,” “source entity” or “data source entity”) that produces requested healthcare information and has a processor and memory allowing it to execute a protocol. *Id.* at 16 (citing Ex. 1005, 17:53–63, 5:12–28; 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 “for producing healthcare information that characterizes a group of a number of individuals identified in a request for the healthcare information that characterizes the group.” Pet. iv. Petitioner cites Evenhaim as disclosing a data server responding to requests for information from an encryption server (data aggregator) by producing healthcare information that characterizes the group, including the de-identified records, e.g., patient records for listed patients, treating physicians, and health outcomes. *Id.* at 16–17 (citing Ex. 1005, Figs. 4, 4A, 5, 8:49–9:12, 12:13–16, 12:42–45, 15:3–14, 15:25–45, 16:8–10; Ex. 1003, Clark Decl. ¶¶ 75–77).

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 “wherein the request for healthcare information is sent to an encryption server that is configured to determine if the number of individuals in the request is at least a defined minimum number of individuals.” Pet. iv. Petitioner cites Evenhaim as disclosing its data aggregator (the claimed encryption server) connects to other machines using standard data communication facilities, such as the Internet. *Id.* at 17–18 (citing Ex. 1005, 12:24–34). Petitioner also notes that Evenhaim discloses that encryption can be performed at numerous locations. *Id.* at 18 (citing Ex. 1005, 12:61–66, 6:57–63; Ex. 1003, Clark Decl. ¶¶ 78–79).

Petitioner notes that Evenhaim’s disclosure that transmitting the parameter list may include transmitting identity-disclosing specifics. Pet. 18 (citing Ex. 1005, 8:13–48, 13:62–65; Ex. 1003, Clark Decl. ¶ 80. Petitioner further cites Evenhaim as disclosing that the number of individuals must be sufficient to protect privacy. *Id.* (citing Ex. 1005, 8:13–48 (“[i]t will simply be necessary that the number of the individuals in any population definition be large enough to dilute any definitive conclusion about an individual’s personal data”), 16:5–32; Ex. 1003, Clark Decl. ¶ 80). According to Petitioner, implementing these requirements by determining whether data for a minimum number of individuals are requested would have been a simple design choice to comply with HIPAA. *Id.* (citing Ex. 1003, Clark Decl. ¶ 80).

Petitioner also argues that it would have been obvious to check that the parameter list is sufficiently large on the aggregator where it is first received, but notes the check could alternatively take place on any of the servers in the system. Pet. 18 (citing Ex. 1003, Clark Decl. ¶ 81; Ex. 1005,

17:53–60, disclosing Evenhaim “allow[s for] either processor to execute characterizing steps of the protocol”).

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 a unique request token is produced for each individual included in the group.” Pet. iv. Petitioner notes that in Evenhaim the parameter list in a request may include individually identifying information, such as names. *Id.* at 19 (citing e.g., Ex. 1005, 6:64–67, 8:18–22; Ex. 1003, Clark Decl. ¶ 82). Petitioner cites Evenhaim as disclosing that after a request for information pertaining to a list of patients, the data aggregator applies an encryption key to those patients and argues that a POSA would understand the data aggregator creates tokens for each individual. *Id.* at 19–20 (citing Ex. 1005, Fig. 4 (steps 1–3); Ex. 1003, Clark Decl. ¶ 82). According to Petitioner, an ordinarily skilled artisan would have understood that the token creation and matching system described in Evenhaim could be applied to the embodiment in Fig. 4 and 4A such that (i) the aggregator would create encrypted tokens from the list of patients received in Fig. 4, box 3, in order to create the query to the data sources in box 4, and (ii) receive back from the data sources de-identified patient data in box 6. *Id.* at 20 (citing Ex. 1005, 12:4–13:20; Ex. 1003, Clark Decl. ¶¶ 84–86). Petitioner further notes Evenhaim’s explanation that token creation could be performed at the aggregator or at the data sources, and states that token creation and matching have been in common use since the 1980’s. *Id.* (citing Ex. 1005, 12:24–34; Ex. 1003, Clark Decl. ¶¶ 82–86; Ex. 1012).

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 “data server is configured to compare the request tokens to tokens associated with healthcare data that includes de-identified information to find matching tokens.” Pet. iv. Petitioner cites Evenhaim as disclosing the use of a one-way hash that creates tokens from identifying information to preserve patient privacy by eliminating the identifying information, while still permitting the linking of records for the same person. *Id.* at 20 (citing Ex. 1005, 12:38–45). According to Petitioner, an ordinarily skilled artisan would have understood that each token produced for a group corresponds to tokens used on data servers to de-identify patient records because Evenhaim describes common encryption across servers for identifying multiple records for the same individual using corresponding tokens. *Id.* at 20–21 (citing Ex. 1005, 12:36–37, 13:1–20; Ex. 1003, Clark Decl. ¶¶ 88–89). Arguing that it would have been obvious to a POSITA to implement the system so each token generated by the aggregator is associated with a token in the data sources that was generated to de-identify the patient records, Petitioner cites Figure 4 of Evenhaim as illustrating that encryption occurs on the aggregator side to produce tokens sent to the data sources to obtain corresponding patient data. *Id.* at 21 (citing Ex. 1003, Clark Decl. ¶¶ 89–92; Ex. 1005, 12:4–13:20, Figs 4 and 4A, as showing how tokens are associated with patient records and how data sources match tokens against de-identified records to find query-responsive data). Petitioner also notes that Evenhaim’s explanation that it was known to de-identify patient records before searching and argues it

would have been obvious that de-identification could occur before or after receipt of a search request. *Id.* (citing Ex. 1003, Clark Decl. ¶¶ 89–91).

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 “the produced healthcare information is absent personally identifiable information.” Pet. iv. Petitioner asserts that Evenhaim’s “produced healthcare information is absent PII because the data is de-identified.” *Id.* at 21 (citing Ex. 1005, 9:13–18 (“deidentified data collection”), 8:49–64, 10:1–6, 12:12–20, 12:35–44, 14:8–13; Ex. 1003, Clark Decl. ¶¶ 93–94).

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

*g) Limitation 7.g*

Petitioner identifies as limitation [7.g] the recitation “is based on a minimum number of matched tokens.” Pet. iv. Petitioner cites both Evenhaim and Murphy as suggesting the requirement for a minimum number of individuals for privacy purposes. *Id.* at 22. Referencing its discussion of limitation [7.c], Petitioner notes that Evenhaim discusses checking for a minimum number of individuals in the request on the encryption server and argues that, because Evenhaim allows for either processor to execute characterizing steps of the protocol, an ordinarily skilled artisan would consider requiring a minimum number of tokens on the data server. *Id.* (citing Ex. 1003, Clark Decl. ¶¶ 95–96; Ex. 1005, 17:53–60). According to Petitioner, it would have been obvious to an ordinarily

skilled artisan “to check both that a minimum number of individuals have been requested and that a minimum number of individuals are returned because of the different vulnerabilities each would protect against in order to comply with HIPAA.” *Id.* (citing Ex. 1003, Clark Decl. ¶¶ 98–99).

Petitioner cites Murphy as disclosing preventing the return of search results with fewer than 3 patients to ensure patient privacy. Pet. 22 (citing Ex. 1009, 555; Ex. 1003, Clark Decl. ¶ 97). According to Petitioner, a person of ordinary skill would have understood “that requiring both a minimum number of individuals in the request on the encryption server and a minimum number of matched tokens on the data server would add protection and further statistical compliance with HIPAA to address known vulnerabilities.” *Id.* (citing Ex. 1003, Clark Decl. ¶¶ 98–99).

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 “the data server is also configured to provide the produced healthcare information to report the characteristics of 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 22 (citing, e.g., Ex. 1005, 10:6–11, 15:3–14, Fig. 4; Ex. 1003, Clark Decl. ¶ 92). Petitioner also cites Evenhaim as disclosing the various types of health information characterizing the group are provided including the de-identified medical records. *Id.* at 23 (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).

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 “absent authorization from the individuals in the group.” Pet. iv. Petitioner cites Evenhaim as disclosing providing healthcare information without authorization at any time from the individuals because it describes de-identification for that purpose under HIPAA. *Id.* at 23 (citing Ex. 1003, Clark Decl. ¶¶ 101–102).

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.

*j) 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 generally correspond to the operations recited in claim 7. *See* Pet. v, 27–30. Claim limitation [1.c] also recites the request message and at least one batch number. Petitioner argues that an ordinarily skilled artisan would have understood “that one way to manage multiple queries and requests, would be

to implement a scheme to identify which query a request is related to, such as including a batch number.” *Id.* at 28 (citing Ex. 1003, Clark Decl. ¶ 115). Petitioner notes that Evenhaim’s disclosure of providing a group name in response to a query concerning Health Programs 1–n at least suggests the use of batch numbers for health programs, study groups or group names because names, batch numbers and other means of identifying groups or programs are interchangeable. *Id.* Petitioner also cites Evanham as disclosing report options and argues that a POSA would have understood the need for different report format options to accommodate different needs of various requesters. *Id.* at 29 (citing Ex. 1005, 8:65–9:12 (describing at least one format option); Ex. 1003 ¶¶ 116–117).

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. *See* Pet. vi–vii, 31–33. 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 15–22*

Claims 2–6 depend from claim 1, claims 8–13 depend from claim 7, claims 15–20 depend from claim 14, and claims 21–22 depend from claim 1. Claims 2, 8, and 15 recite that the provided healthcare information is in conformity with HIPAA. Referencing its analysis of limitation [7.i], Petitioner cites Evenhaim as being directed to such information. *See, e.g.*, Pet. 23; *see also* Ex. 1005, 1:58–62, 2:5–57.

Claims 3, 9, and 16 recite that the request for healthcare 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, e.g.*, Pet. 23 (citing Ex. 1005, 12:38–45, 12:8–16; 13:62–14:13, 8:39–43; Ex. 1003 Clark Decl. ¶ 103).

Claims 4, 10, and 17 recite that the data identifying each individual is encrypted. Petitioner cites Evenhain as disclosing this feature. *See, e.g.*, Pet. 23–24 (citing, e.g., Ex. 1005, Fig. 4, 12:4–13:20; Ex. 1003, Clark Decl. ¶ 104). Claims 5, 11, and 18 recite that the tokens associated with the healthcare data and the request tokens are similarly encrypted. Petitioner cites Evenhain’s use of a common encryption key to ensure that records for the same patient can be matched as disclosing this feature. *See id.* at 23–34 (citing Ex. 1005, 12:4–16, 12:25–30, 12:39–44, 16:46–57, 17:27–41; Ex. 1003, Clark Decl. ¶¶ 107–108).

Claims 6, 13, and 19 recite that the healthcare data represents medical related information associated with individual of the group. Petitioner cites Evenhain as disclosing the medically related data includes patient-level microdata and is associated with individuals of the group. *See* Pet. 23–34 (citing Ex. 1005, Figs. 1, 2, 5; 10:46–54, 11:14–29, 12:36–47, 16:46–57, 17:27–41; Ex. 1003, Clark Decl. ¶¶ 27, 110).

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] as demonstrating that Evenhain and Murphy in combination disclose this feature. *See* Pet. 25, 34.

Claim 21 depends from claim 1 and recites that the identity of the individuals is unattainable from the unique request token. Petitioner cites its discussion of limitations [7.f] and [7.g] as demonstrating that Evenhain and Murphy in combination disclose this feature. Pet. 34.

Claim 22 depends from claim 1 and recites the unique request token and the tokens associated with the healthcare data are similarly encrypted. Petitioner cites its discussion of claim 11 as demonstrating that Evenhaim and Murphy in combination disclose this feature. Pet. 35.

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 15–22 to a person of ordinary skill in the art.

*C. Petitioner’s Contentions That Claims 1–22 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.

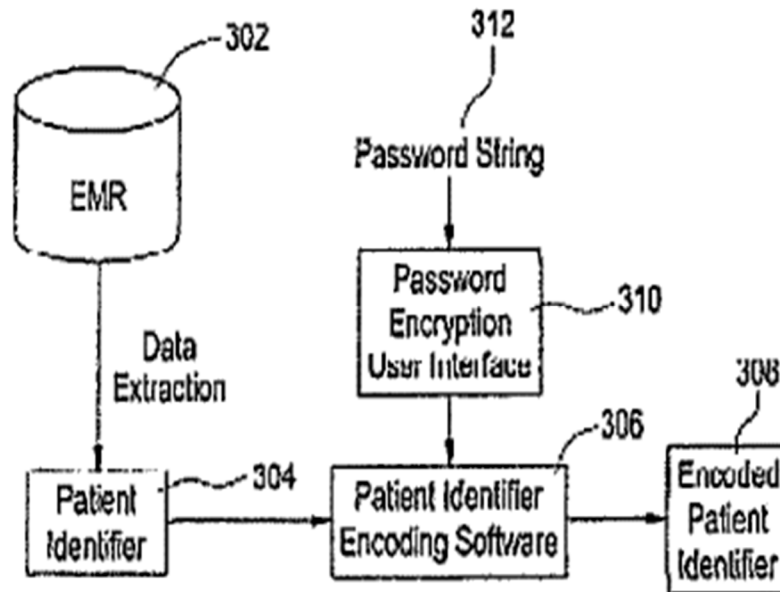


Figure 3 is a block diagram illustrating a process for de-identifying patient data during data extraction for transmission to a data warehouse. Ex. 1006 ¶ 38. Patient data extracted from an electronic medical record (EMR) database 302 and personal identifying information is “removed or transformed in 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. 37 (citing Ex. 1005, 15:15–24, 16:5–21, Fig 4; Ex. 1006, Figs. 1–2, ¶ 27; Ex. 1003, Clark Decl. ¶ 150). 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. ¶ 149). 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 36–37 (citing Ex. 1006 ¶¶ 37–43; Ex. 1003, Clark Decl. ¶¶ 47, 51–52, 148–149).

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. Pet. 38 (citing Ex. 1006 ¶¶ 9, 14, 17, 27, 39–40; Ex. 1003, Clark Decl. ¶¶ 148–149). 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. *See* Pet. 37–39.

### 3. *Analysis of Representative Claim 7*

As to the subject matter identified by Petitioner as limitations [7.a–7.i], Petitioner cites the teachings of Evenhaim as discussed previously. Pet. 39–45. Petitioner further discusses Settimi’s disclosure concerning several specific limitations. *Id.*

As to limitation [7.b] (producing healthcare information that characterizes a group . . . identified in a request), Petitioner also notes that in Evenhaim, tokens are created in step 3 in Figure 4 before being sent to the repository; in combination with Settimi, the query would be sent to a central warehouse that contains only de-identified records in which PII has been replaced with an encrypted token, rather than being sent to each individual source (e.g., a health plan). Pet. 39–41 (citing, e.g., Ex. 1005, Fig. 4, 12:4–13:20, 8:18–22; Ex. 1006 ¶¶ 35, 37; Ex. 1003, Clark Decl. ¶¶ 157–158).

As to limitation [7.d] (wherein a token is produced for each individual), Petitioner also states that in Evenhaim, each data source in Figure 4 (PBM 1–n) would de-identify its patient records by creating an encrypted token and in combination with Settimi and would send the de-identified patient records to a central warehouse. Pet. 41 (citing Ex. 1003, Clark Decl. ¶ 161). Petitioner further argues that, based on Evenhaim’s encrypted patient list, an ordinarily skilled artisan would have understood to use an encryption that allows for finding matching records in Settimi’s central warehouse, such that a query consisting of a list of encrypted tokens

would be sent to the central warehouse that contains corresponding matching tokens for de-identified patient data. *Id.* at 41–43 (citing Ex. 1005, Fig. 4, 12:4–13:20; Ex. 1003, Clark Decl. ¶¶ 162–164).

As to limitation [7.e] (comparing request tokens to tokens to find matching tokens), Petitioner notes that in Settimi, each token produced in a query corresponds to a token in the de-identified information in the central warehouse, such that creating patient cohort reports based on querying longitudinal patient data is supported by the ability to connect all records relating to a single patient in the data warehouse. Pet. 43 (citing Ex. 1006 ¶¶ 27, 30, 35–37, 39–42; Ex. 1003, Clark Decl. ¶ 166). Petitioner observes that no names or other PII could be used in the query in Settimi because the centralized warehouse has no such information, and argues 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 44 (citing Ex. 1003, Clark Decl. ¶ 168; Ex. 1006 ¶ 37).

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 generally correspond to the operations recited in claim 7. *See* Pet. 46–48.

As to limitation [1.c], Petitioner cites its discussion of claim 1 in its challenge based on Evenhaim and Murphy. *Id.* at 47.

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 15–22*

Claims 2–6 depend from claim 1, claims 8–13 depend from claim 7, claims 15–20 depend from claim 14, and claims 21–22 depend from claim 1. Petitioner contends that claims 2–6, 8–13, and 15–22 are unpatentable for essentially the same reasons as those Petitioner articulated in its arguments concerning Evenhaim and Murphy. Pet. 48–52.

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 15–22 to a person of ordinary skill in the art.

D. *Petitioner’s Contention That Claims 1–22 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 first server sends a query that characterizes the group to a second server request (medical repository) that returns de-identified healthcare information in response to the query.” Pet. 52 (citing Ex. 1007, code (57), ¶ 24, claim 23; Ex. 1003, Clark Decl. ¶¶ 54, 200). 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.* (citing Ex. 1007 ¶¶ 13, 44–46; Ex. 1003, Clark Decl. ¶ 213).

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. Pet. 53 (citing Ex. 1003, Clark Decl. ¶¶ 213–214). 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 “Encrypted IDs” created using a common, freely distributable, public key to facilitate a token matching system used to locate medical records, such as those in Dick. *Id.* at 54–57 (citing Ex. 1003, Clark Decl. ¶¶ 216–219; Ex. 1007 ¶¶ 11, 24–25). Petitioner further argues an ordinarily skilled artisan would have had reason to combine the teachings of Dick and Landi with Murphy’s teaching to prevent returning too few results in order to preserve patient privacy, thereby achieving a goal that is common to Dick, Landi, and HIPAA. *Id.* at 57 (citing Ex. 1003, Clark Decl. ¶¶ 221–222).

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.

#### 4. *Analysis of Representative Claim 7*

As to claim limitations [7.a] (a system comprising a data server) and 7[b] (producing healthcare information that characterizes a group . . . identified in a request), Petitioner cites Figure 3 of Dick as disclosing physical embodiments of a data server device for producing such healthcare information in the form of a Medical Information Repository. Pet. 58–59 (citing Ex. 1003, Clark Decl. ¶¶ 223–226); *see also* Ex. 1007 ¶¶ 19–22, 24,

32, 44–46, disclosing a system in which Requester’s Server 230 receives a request from a “requesting and viewing client[]” (RVC) to obtain from a Medical Information Repository (central server 245) medical records for a subject that may be a human individual or a group of humans). Petitioner cites Landi as disclosing an alternative networked computer system with a central database (data server) storing de-identified records, i.e., records in which PII has been replaced with tokens (Encrypted IDs) for healthcare information regarding an individual or a group, that shares those records in response to third party queries. Pet. 59 (citing Ex. 1008, 7:3–31, 8:16–55, 10:52–65). Petitioner contends that a person of ordinary skill would have understood that Landi’s manner of storing de-identification data could be used with or in place of Dick’s repository. *Id.* (citing Ex. 1003, Clark Decl. ¶ 226).

As to limitation [7.c] (the request . . . is sent to an encryption server . . . configured to determine if the number of individuals in the request is at least a defined minimum number), Petitioner cites Dick as describing Requester’s Server 230 that receives names of a group of individuals from a client (RVC), creates a query, and in connection with central server 245 transmits the query for HIPAA compliant de-identified healthcare information to a Medical Information Repository. Pet. 59 (citing Ex. 1007, Fig. 3, ¶¶ 22, 24, 28, 34, claim 23; Ex. 1006 ¶¶ 44–46; Ex. 1003, Clark Decl. ¶ 227). Citing Landi as describing a processing system that uses encryption to create tokens from PII using a public encryption key, Petitioner contends that an ordinarily skilled artisan would implement Landi’s processing system on Dick’s requester server because Dick contemplates the use of de-identifying methods and processes to comply with HIPAA. *Id.* at 60 (citing Ex. 1007 ¶ 46; Ex. 1003, Clark Decl. ¶ 55). Petitioner further contends that

it would have been obvious to a POSA to implement techniques that prevent a searcher from matching a particular medical record to a particular person, including by ensuring data about a minimum number of individuals is requested. *Id.* at 60–61 (citing Ex. 1003, Clark Decl. ¶¶ 66, 230–233).

As to limitation [7.d] (a token is produced 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. 62 (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 62–63. Petitioner argues that this correspondence facilitates matching request tokens to medical data tokens, as in limitation [7.e], which recites that the data server is configured to compare tokens to find matching tokens. *Id.* at 63–65 (citing Ex. 1008, Fig. 3, 8:38–55, 11:23–29; Ex. 1003, Clark Decl. ¶¶ 240–241). Petitioner further cites Landi as disclosing the produced information is absent PII, as recited in limitation [7.f], because it is de-identified. *Id.* at 65 (citing Ex. 1008, 5:32–47, 2:30–54, 13:41–53, 2:5–26; Ex. 1003, Clark Decl. ¶¶ 245–246).

As to limitation [7.g] (the information is based on a minimum number of matched tokens), Petitioner argues that Dick describes using statistical

methods to ensure an individual's medical records are not identified and one well-known method of de-identification not mentioned in Dick is preventing the return of one record that can be associated with a particular patient based on the search parameters. Pet. 65 (citing Ex. 1007 ¶ 46; Ex. 1003, Clark Decl. ¶¶ 247–249). Petitioner further cites Murphy as disclosing an algorithm that facilitates HIPAA compliance by preventing the return of fewer than 3 token matched patient records so that, even absent PII, an individual patient cannot be identified. *Id.* at 65–66 (citing Ex. 1009, 555; Ex. 1003, Clark Decl. ¶¶ 66, 250–251).

As to limitations [7.h] (the data server is configured to provide the produced healthcare information) and [7.i] (absent authorization from the individuals), Petitioner cites Dick as disclosing that in some instances the law does not require obtaining releases from individuals and Landi as disclosing HIPAA allows certain entities to supply de-identified data for certain purposes, without being subject to privacy rules. Pet. 66–67 (citing Ex. 1007 ¶¶ 24, 26, 47; Ex. 1008, 1:5–18; Ex. 1003, Clark Decl. ¶¶ 253–255).

#### 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. *See* Pet. 69–72. Petitioner

notes that limitation [1.c] also recites that the request message includes a batch number and at least one report option. *Id.* at 70. Petitioner notes Dick’s explanation that each request can include an identifier for a group of individuals. *Id.* (citing Ex. 1007 ¶ 24 (“[e]ach request for medical information includes identification of a subject . . . . A subject might consist of a . . . group of humans.”)). Petitioner contends that an ordinarily skilled artisan would have understood that the subject identifier could be a batch number. *Id.* (citing Ex. 1003, Clark Decl. ¶ 266). Petitioner further contends an ordinarily skilled artisan would have understood that assigning batch numbers to queries is one way to manage multiple information requests for healthcare information from multiple requesters using multiple encryption servers and data servers. *Id.* (citing Ex. 1007 ¶¶ 29–30, 32; Ex. 1003, Clark Decl. ¶ 266). Noting that Dick recognizes that requests for medical information will come from many different sources for many different reasons and that the server can provide functions that add value, Petitioner also argues that a POSA would recognize different report options could be provided, as claimed. *Id.* at 70–71 (citing Ex. 1007 ¶ 34; Ex. 1003, Clark Decl. ¶ 267).

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. *See* Pet. 73–74. 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 15–22*

Claims 2–6 depend from claim 1, claims 8–13 depend from claim 7, claims 15–20 depend from claim 14, and claims 21–22 depend from claim 1.

Claims 2, 8, and 15 recite that the provided information is medical information in conformity with HIPAA. Petitioner cites its discussion on limitation [7.b] in asserting that Dick discloses producing de-identified medical information. Pet. 67.

Claims 3, 9, and 16 recite that the request for healthcare information that characterizes a group of individuals includes PII associated with those individuals. Petitioner cites its discussion of limitation [7.d], which addresses Dick's description of a request for healthcare information including the identification of a subject that may be a human individual or group of humans, which is PII, and Landi's central medical record database of de-identified information. Pet. 61, 67.

Claims 4, 10, and 17 recite that the data identifying each individual is encrypted. Petitioner cites its discussion of limitation [7.b]. Pet. 67. We note, however, that Petitioner's discussion of limitation [7.d] cites Landi's Encrypted IDs (a unique reproducible encrypted version of patient identifying information, that preserves patient uniqueness to enable to the same patient to be recognized) as disclosing this limitation. *Id.* at 61–62. Claims 5, 11 and 18 recite that the tokens associated with the healthcare 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.* at 67–68 (citing Ex. 1008, 8:47–55, 11:3–29, 4:65–5:2).

Claims 6, 13, and 19 recite that the healthcare data represents medical-related information associated with individuals of the group. Petitioner cites Dick as disclosing the query for Dick's Request Server is for medically related information that characterizes a group of individuals. Pet. 68–69. 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 69.

Claims 12 and 20 recite that producing the requested information includes determining if the group includes a minimum number of individuals. Petitioner cites Murphy as disclosing an algorithm that, in compliance with HIPAA, blocks returning information on fewer than 3 patients in response to a query. Pet. 68 (citing Ex. 1009, 555; Ex. 1003, Clark Decl. ¶¶ 66, 261).

Claim 21 depends from claim 1 and recites that the identity of the individuals is unattainable from the unique request token. Petition cites its discussion of limitations [7.f.] and [7.g] as demonstrating that Dick, Landi, and Murphy in combination disclose this feature. Pet. 75.

Claim 22 depends from claim 1 and recites the unique request token and the tokens associated with the healthcare data are similarly encrypted. Petitioner cites its discussion of claim 11 as demonstrating that Dick, Landi, and Murphy in combination disclose this feature. Pet. 76.

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 15–22 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 1–22 in the '375 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

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

IPR2024-00311  
Patent 10,109,375 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