

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DATAVANT, INC.,
Petitioner,

v.

VIGILYTICS LLC,
Patent Owner.

IPR2024-00226
Patent 9,118,641 B1

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

GIANNETTI, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Background

Datavant, Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1–19 (the “challenged claims”) of U.S. Patent No. 9,118,641 B1 (Ex. 1001, the “’641 patent”). Paper 1 (“Pet.”), 2. Vigilytics LLC (“Patent Owner”) has not filed a preliminary response.

For the reasons stated below, we determine that Petitioner has established a reasonable likelihood that it would prevail with respect to at least one claim. *See* 35 U.S.C. § 314(a) (2018) (*inter partes* review may not be instituted unless “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition”). We therefore institute *inter partes* review as to all of the challenged claims of the ’641 patent and all asserted grounds of unpatentability. *See SAS Inst. Inc. v Iancu*, 138 S. Ct. 1348, 1356 (2018); 37 C.F.R. § 42.108(a) (2023) (“When instituting *inter partes* review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.”).

B. Related Proceedings

The parties identify the following district court proceeding as involving the ’641 patent: *Milliman, Inc. et al. v. Gradient AI Corp. et al.*, No. 1:21-cv-10865 (D. Mass.). Pet. 1; Paper 4, 1.

The following other pending petitions for *inter partes* review filed by Petitioner involve patents related to the ’641 patent: IPR2024-00307, filed Dec. 15, 2023 (U.S. Patent No. 9,965,651); IPR2024-00311, filed Dec. 15, 2023 (U.S. Patent No. 10,109,375); IPR2024-00381, filed Jan. 4, 2024 (U.S.

Patent No. 10,886,012); IPR2024-00382, filed Jan. 4, 2024 (U.S. Patent No. 9,665,685).

C. Real Parties-in-Interest

Petitioner identifies the following real parties-in-interest: “Datavant, Inc. and Ciox Health LLC.” Pet. 1. Patent Owner identifies only itself, “Vigilytics LLC,” as the real party-in-interest. Paper 4, 1.

D. The '641 Patent

The '641 patent is titled “De-Identifying Medical History Information for Medical Underwriting.” Ex. 1001, (54). The patent “relates to processing and transmitting personal data, the dissemination of which is restricted by federal law.” *Id.* at 1:14–16. Specifically, the patent relates to “de-identifying [of] medical history information.” *Id.* at 1:40–41.

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, 1:42–45. The identity of the individuals is unattainable from the produced information. *Id.* at 1:45–46. The method also includes providing the produced information to report the characteristics of the group. *Id.* at 1:46–48.

This operation is illustrated in Figure 3 of the '641 patent, reproduced below.

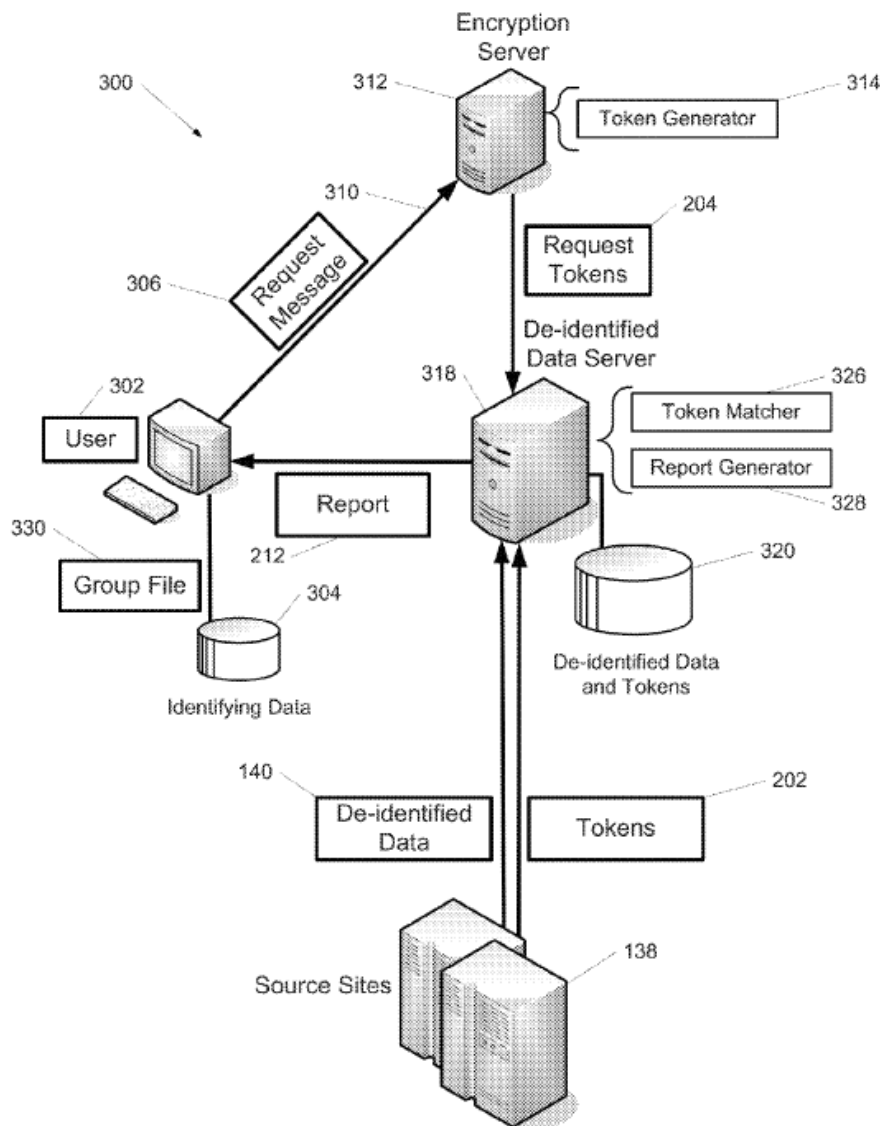


Figure 3 “illustrates an exemplary system incorporating an encryption server and a de-identified data server to enable a user who is not permitted to obtain the private data of a group of people to instead obtain a report that characterizes the group as a whole.” Ex. 1001, 3:5–9. In operation, request message 306 is sent over communications network 310 (e.g., the Internet) to encryption server 312. *Id.* at 5:31–33. If the request message contains a minimum number of group members, encryption server 312 creates a unique token, or identifier, for each person in the message 306. *Id.* at 5:33–36.

The encryption server creates each token by applying token generator 314 that encrypts the personally identifiable information of each group member. Ex. 1001, 5:36–38. 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 5:40–43.

Encryption server 312 provides request tokens 204 to de-identified data server 318. Ex. 1001, 5:44–45. The de-identified data server 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 5:44–49. Each token obtained from the source sites 138 has 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 5:49–53.

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, 6:1–4. All available data for matched tokens, the requested de-identified data 208, is retrieved for use in report generator 328. *Id.* at 6:4–6.

E. Illustrative Claim

The Petition challenges claims 1–19, of which claims 1, 7, and 14 are independent. Claim 7 is illustrative of the claimed subject matter and is reproduced below:

7[a]. A system comprising: an encryption server, having a processor and a memory,

- [b] for producing a token for each individual included in a group composed of multiple individuals identified in a request for healthcare information that characterizes the group,
- [c] wherein the identity of the individuals in the group is unattainable from the tokens, each token being associated with a corresponding token in a set of de-identified healthcare data,
- [d] and each token in the set of de-identified healthcare data being associated with healthcare data for a corresponding individual;
- [e] a data server for producing the requested healthcare information that characterizes the group
- [f] by identifying the tokens in the set of de-identified healthcare data and the associated de-identified healthcare data that correspond to the produced tokens,
- [g] wherein the produced tokens and the tokens in the set of de-identified data are similarly encrypted,
- [h] and the produced healthcare information is absent personally identifiable information
- [i] and has been produced without the individuals in the group having authorized production of such healthcare information that characterizes the group; and
- [j] providing the produced healthcare information to report the characteristics of the group composed of multiple individuals
- [k] absent authorization at any time from the individuals in the group of individuals to provide the requested healthcare information.

Ex. 1001, 11:8–35.¹ Claim 1 is directed to a computer-implemented method and claim 14 recites a non-transitory storage medium and are directed to subject matter similar to claim 7. *Id.* at 10:25–54, 12:1–32.

¹ Paragraph identifiers in brackets have been added.

F. References and Other Evidence

The Petition relies on the following references:

Name	Reference	Publication/ Issue Date	Exhibit
Evenhaim	US 7,823,207 B2	Oct. 26, 2010	Ex. 1005
Settimi	US 2007/0294111 A1	Dec. 20, 2007	Ex. 1006
Dick	US 2002/0111833 A1	Aug. 15, 2002	Ex. 1007
Landi	US 7,519,591 B2	Apr. 14, 2009	Ex. 1008
Murphy	Shawn N. Murphy et al., <i>A Security Architecture for Query Tools Used to Access Large Biomedical Databases</i> , 2002 AMIA Annual Symposium Proceedings, 552–56 (2002)	Nov. 9–13, 2002	Ex. 1009

In addition, Petitioner submits the Declaration of Paul C. Clark (Ex. 1003, “Clark Decl.”).

G. Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims are unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §²	Reference(s)/Basis
1–19	103	Evenhaim
1–19	103	Evenhaim, Settimi
7–10, 13	103	Dick, Landi
1–6, 11, 12, 14–19	103	Dick, Landi, Murphy

See Pet. 9.

H. Overview of the Prior Art

1. Evenhaim (Ex. 1005)

Evenhaim is titled “Privacy Preserving Data Mining Protocol.” Ex. 1005, (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

² Because the earliest application from which the ’641 patent claims priority was filed before March 16, 2013, the pre-AIA (“America Invents Act”) versions of §103 applies. Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011).

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, 6:48–56.

This is illustrated in Evenhaim’s Figure 4, reproduced below.

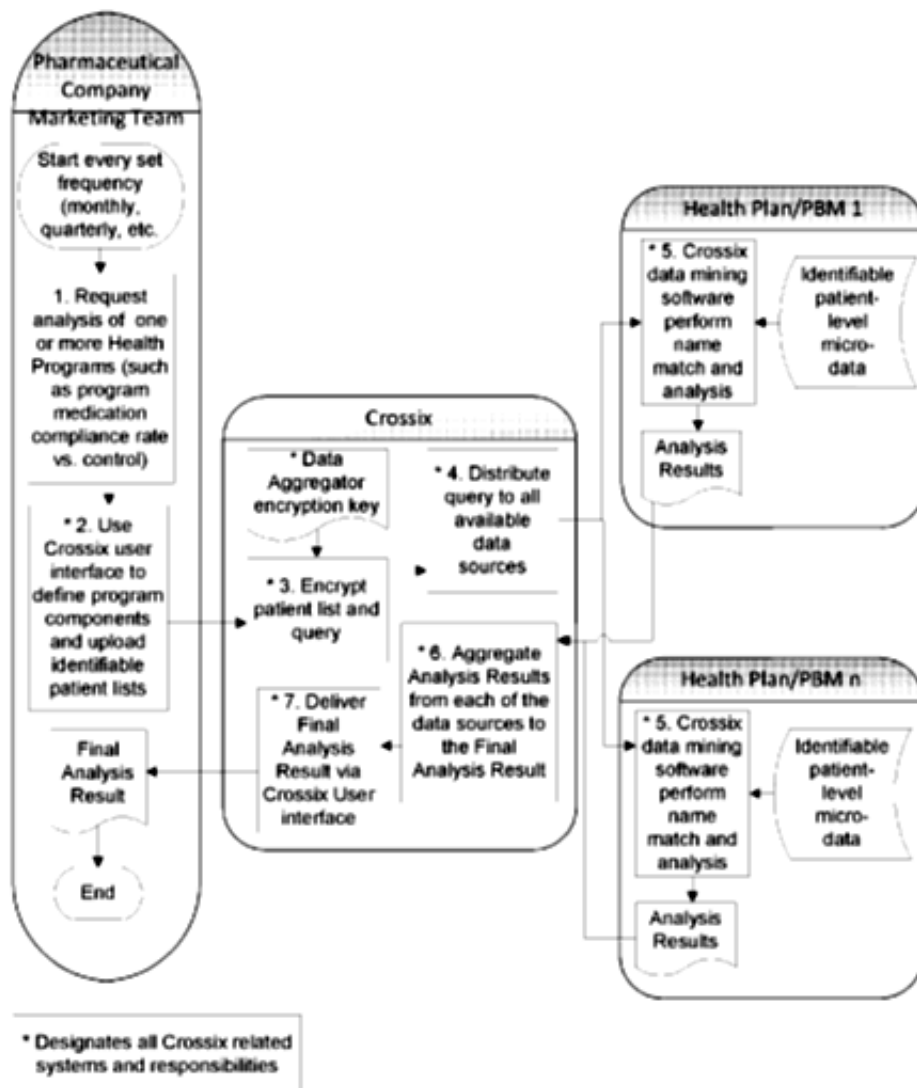


FIG. 4

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 given 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, 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. Settimi (Ex. 1006)

Settimi is titled “Systems and Methods for Identification of Clinical Study Candidates.” Ex. 1006, (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 describes also “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.

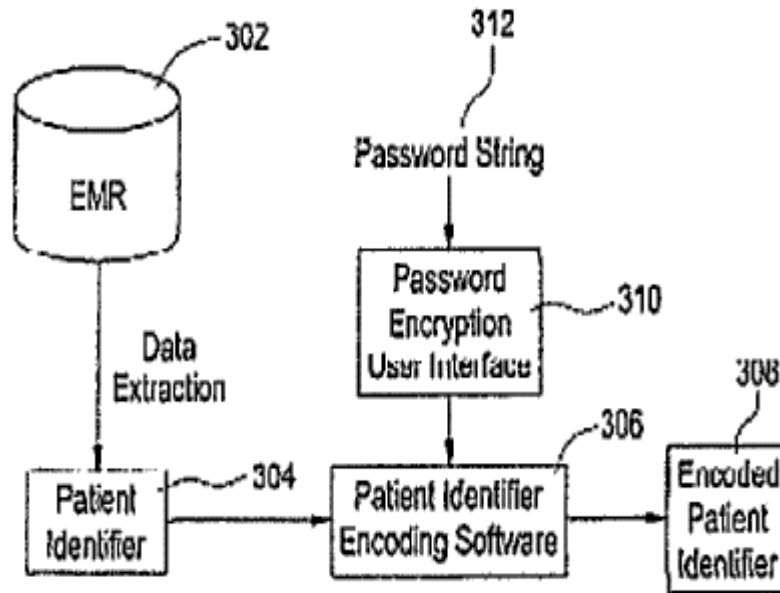


Figure 3 is a block diagram illustrating a process for de-identifying patient data during data extraction for transmission to a data warehouse. Ex. 1006 ¶ 38. Patient data extracted from an electronic medical record (EMR) database 302 and personal identifying information is “removed or transformed in 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.

3. Dick (Ex. 1007)

Dick is titled “Method and Apparatus for Requesting and Retrieving De-Identified Medical Information.” Ex. 1007, (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 a given example, the interacting entities are “requesting and viewing clients” (RVC), a central server, and medical information repositories. Ex. 1007 ¶¶ 20, 27–28. A request for medical information is sent by an RVC to the central server 245, includes a person or group of persons identified by name(s) (or the like), and 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.

4. Landi (Ex. 1008)

Landi is titled “Systems and Methods for Encryption-based De-Identification of Protected Health Information.” Ex. 1008, (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.

5. Murphy (Ex. 1009)

Murphy describes a server application of “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.

II. ANALYSIS OF THE CHALLENGED CLAIMS

A. Level of Ordinary Skill in the Art

Petitioner contends a person of ordinary skill in the art of the '641 patent would have possessed “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 Clark Decl. ¶ 22). Petitioner adds that “[s]uperior education could compensate for less work experience, and vice-versa.” *Id.*

We regard Petitioner’s description as consistent with the prior art before us. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (prior art itself may reflect an appropriate level of skill). Thus, for the purpose of our decision, we adopt Petitioner’s proposal.

B. Claim Construction

We construe claim terms only as relevant to the parties’ contentions and only to the extent necessary to resolve the issues in dispute. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

Petitioner identifies Patent Owner’s constructions for several terms³ from Patent Owner’s claim-construction brief in the related district court litigation and “adopts these constructions for this proceeding.” Pet. 8 (citing Ex. 1010, 9–20). Patent Owner’s brief identifies these as “disputed claim terms.” Ex. 1010, i (Table of Contents). The brief indicates that Petitioner disputes Patent Owner’s construction for each of the terms. *Id.* at 1 (referring to the parties’ Joint Claim Construction Statement).

As Petitioner expressly “adopts these constructions for this proceeding” (Pet. 8), we understand these constructions to be Petitioner’s identification of “[h]ow the challenged claim is to be construed” under 37 C.F.R. 42.104(b)(3) (2023). 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.*, 868 F.3d at 1017. 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.

C. Obviousness – General

A claim is unpatentable as obvious under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said

³ These are “token,” “server,” “encryption server,” “similarly encrypted,” “medical information that characterizes the group,” and “absent authorization” terms. Ex. 1010, i.

subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called “secondary considerations,” including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). At this stage, neither party has presented any evidence on the fourth *Graham* factor.

D. Obviousness – Evenhaim Alone

Petitioner contends that claims 1–19 would have been obvious over Evenhaim. Pet. 9. As Patent Owner has not filed a preliminary response, these contentions are uncontested at this stage.

1. Claim 7

Petitioner asserts that Evenhaim teaches or suggests each limitation of independent claim 7 and provides an element-by-element analysis supported by testimony from Dr. Clark. Pet. 10–34; Clark Decl. ¶¶ 67–84.

Petitioner contends element 7[a] (“... an encryption server, having a processor and a memory”) is met by Evenhaim’s teachings of a “data aggregator.” Pet. 14–15 (citing Clark Decl. ¶¶ 68–69).⁴

⁴ This first element includes the claim’s preamble (“[a] system”). We do not express an opinion as to whether the preambles of the challenged claims are limiting.

Petitioner contends that element 7[b] (“producing a token for each individual included in a group . . .”) is met by Evenhaim’s teachings of a data aggregator that “produces a token (unique encryption key) for each individual in a group.” Pet. 15–17 (citing Ex. 1005, Fig. 4, 12:4–13:20); Clark Decl. ¶¶ 70–74. Petitioner contends that “after a request for information pertaining to a list of patients, the data aggregator applies an encryption key to encrypt those patients.” Pet. 17.

For element 7[c] (“wherein the identity of the individuals in the group is unattainable from the tokens, each token being associated with a corresponding token in a set of de-identified healthcare data,”), Petitioner identifies Evenhaim’s teachings “that the identity of the individuals is unattainable from the tokens.” Pet. 17–18. Petitioner explains that “Evenhaim uses, e.g., a one-way hash that creates the tokens from PII, which preserves the privacy of the patient by eliminating the PII, but still allows linking records for the same person.” *Id.* at 17 (citing Ex. 1005, 12:38–45); Clark Decl. ¶¶ 75–77.

To meet element 7[d] (“each token in the set of de-identified healthcare data being associated with healthcare data for a corresponding individual”) Petitioner cites Evenhaim’s teachings “that each token is de-identified personal data associated with that individual’s healthcare records.” Pet. 18–19; Clark Decl. ¶¶ 78–80.

Petitioner contends that element 7[e] (“a data server for producing the requested healthcare information that characterizes the group”) is met by Evenhaim’s teachings of the data server called “data source,” “source entity,” or “data source entity.” Pet. 19–20; Clark Decl. ¶¶ 81–84.

Petitioner contends that element 7[f] (“identifying the tokens in the set of de-identified healthcare data and the associated de-identified healthcare data that correspond to the produced tokens”) is met by Evenhaim’s teachings of “tokens in the form of unique encryption keys created from PII using a one-way hash.” Pet. 20–24; Clark Decl. ¶¶ 85–87.

Petitioner contends that element 7[g] (“wherein the produced tokens and the tokens in the set of de-identified data are similarly encrypted”) is met by Evenhaim’s teaching “that the produced tokens from the aggregator and tokens in the de-identified data on the data sources are similarly encrypted.” Pet. 24–25 (citing Ex. 1005, 12:4–16); Clark Decl. ¶¶ 88–89.

Elements 7[h] and 7[i] both address the produced healthcare information. Pet. iv. Element 7[h] states that “the produced healthcare information is absent personally identifiable information.” *Id.* Element 7[i] states that “the produced healthcare information . . . has been produced without the individuals in the group having authorized production of such healthcare information that characterizes the group.” *Id.* Petitioner contends that these limitations are met by Evenhaim’s teachings that “the data is de-identified.” *Id.* at 25 (citing Ex. 1005, 9:13–18); Clark Decl. ¶¶ 90–92. Petitioner explains that “[a] purpose of Evenhaim is to produce de-identified healthcare information that can be released to third parties without individuals in the group authorizing the release, to comply with HIPAA.” Pet. 25.

Petitioner contends that element 7[j] (“providing the produced healthcare information to report the characteristics of the group composed of multiple individuals”) is met by Evenhaim’s teaching of “healthcare

information reports” produced by the aggregator. Pet. 25–26 (citing Ex. 1005, Figs. 4–5); Clark Decl. ¶ 93.

Petitioner contends that element 7[k] (“providing the produced healthcare information . . . absent authorization at any time from the individuals in the group of individuals . . .”) is met by Evenhaim’s teaching to “provide[] the healthcare information without authorization ‘at any time’ from the individuals” and “under HIPAA.” Pet. 26 (citing Clark Decl. ¶ 94).

At this stage, Patent Owner does not dispute any of these contentions. We find that for the reasons given by Petitioner and supported by testimony from Dr. Clark, Petitioner has demonstrated a reasonable likelihood of prevailing on this obviousness challenge to claim 7 based on Evenhaim.

2. Claims 1–6 and 8–19

Claims 2–6 depend from claim 1. Claims 8–13 depend from claim 7. Claims 15–19 depend from claim 14. Petitioner asserts claims 1–6 and 8–19 would have been obvious over Evenhaim and provides an element-by-element analysis for each claim. Pet. 29–34; Clark Decl. ¶¶ 95–133.

For independent claims 1 and 14, Petitioner relies on its analysis of claim 7, discussed *supra*. See Pet. 29–31 (claim 1), 32–33 (claim 14).

At this stage, Patent Owner does not dispute these contentions. We find that for the reasons given by Petitioner and supported by testimony from Dr. Clark, Petitioner has demonstrated a reasonable likelihood of prevailing on these obviousness challenges to claims 1–6 and 8–19 based on Evenhaim.

3. Summary

For the reasons given, Petitioner has demonstrated a reasonable likelihood of prevailing on its challenges to claims 1–19 based on Evenhaim.

E. Obviousness – Evenhaim and Settimi

Petitioner asserts that Evenhaim and Settimi teach or suggest each limitation of claims 1–19 and provides an element-by-element analysis supported by testimony from Dr. Clark. Pet. 34–50; Clark Decl. ¶¶ 134–198. As Patent Owner has not filed a preliminary response, these contentions are uncontested at this stage.

Dr. Clark testifies that a person of ordinary skill would have been motivated to combine the teachings of these references with a reasonable expectation of success. Clark Decl. ¶¶ 135–138. For example, he testifies that “a [person of ordinary skill] would look to combine Evenhaim’s distribution system and ability to query healthcare data with the centralized server of de-identified patient data taught by Settimi to streamline the process of querying the data sources in Evenhaim.” *Id.* ¶ 135. He testifies that “[a person of ordinary skill] would find that Settimi’s centralized warehouse of de-identified patient data would be a more convenient and reliable way to update data and obtain complete responses to the query for healthcare information.” *Id.* ¶ 136.

Petitioner’s analysis for this challenge draws upon its analysis of the obviousness ground based on Evenhaim alone, discussed *supra* in Section II.D. *See, e.g.*, Pet. 37–40 (analyzing claim elements 7[a]–7[e], each referring to corresponding limitations in “Ground 1” (obviousness over Evenhaim alone)).

We have already determined in Section II.D that Petitioner has demonstrated sufficiently at this stage that claims 1–19 would have been obvious over Evenhaim alone. For the reasons given, we determine that Petitioner has also demonstrated a reasonable likelihood of prevailing on these challenges to those claims based on Evenhaim and Settimi.

F. Obviousness – Dick and Landi and Dick, Landi, and Murphy

Petitioner contends claims 7–10 and 13 would have been obvious over Dick and Landi and claims 1–6, 11, 12, and 14–19 would have been obvious over those references further in light of Murphy. Pet. 9. At this stage, these contentions are uncontested.

1. Claim 7

Petitioner asserts that Dick and Landi teach or suggest each limitation of independent claim 7 and provides an element-by-element analysis. Pet. 55–66. Dr. Clark provides supporting testimony. Clark Decl. ¶¶ 207–229.

Petitioner demonstrates that each claim limitation is met by Dick and Landi. For example, Petitioner contends element 7[a] (“an encryption server, having a processor and a memory”) is met by Dick’s teachings of a “requester’s server . . . that receives the names of a group of individuals . . . and then creates a query that it transmits . . . to a Medical Information Repository.” Pet. 55 (citing Ex. 1007, Fig. 3, ¶¶ 22, 28, 34, claim 23) (capitalization and internal quotations omitted); Clark Decl. ¶ 207. Petitioner also contends that Landi teaches using “processors” and “program storage devices” to create tokens from PII via a public encryption key. Pet. 55; Clark Decl. ¶¶ 208–209.

Petitioner contends also that element 7[b] (“for producing a token . . .”) is met by Dick’s teachings that the “Requester’s Server (encryption server) receives a request for medical records for a ‘subject’” and Landi’s teachings that “central database/system 30 contain[s] medical records for searching includes solely de-identified records in which PII has been replaced with a token in the form of Encrypted IDs for each individual that has patient records.” Pet. 55–56 (*see* Clark Decl. ¶¶ 210–213).

Dr. Clark testifies that there would have been a motivation to combine these teachings with an expectation of success. Clark Decl. ¶¶ 203–206. He testifies that “Landi’s detailed disclosure on how to created encrypted tokens from identifying information using the same or similar public encryption keys fits perfectly into Dick’s system for producing de-identified healthcare information that characterizes a group of individuals, and would work well for accomplishing the examples described in Dick.” *Id.* ¶ 206; *see also id.* ¶¶ 214–215.

Petitioner contends that element 7[c] (“identity of the individuals . . . is unattainable from the tokens . . .”) is met by Landi’s teachings to de-identify PII into tokens (Encrypted IDs). Pet. 58–59; Clark Decl. ¶¶ 216–218. Dr. Clark testifies that “[t]he identity of the individuals that correspond to the tokens (Encrypted IDs) described in Landi, and implemented on Dick’s Requester Sever, are not obtainable from the tokens absent a private key which must be used to decrypt the identifying data and is described as only being accessible to an authorized party.” Clark Decl. ¶ 216. He continues, “Dick in view of Landi also describes or suggests that each produced token can be associated with a corresponding token in a set of de-

identified healthcare data stored in the central data repository, the Medical Information Repository.” *Id.* ¶ 217.

In Landi, the medical records from the various sources are de-identified, before being sent to the central repository, by encrypting the PII of the individual to create a token and removing the PII. Pet. 58 (citing Ex. 1008, 4:11–28, 5:32–44). Further, the purpose of disseminating a public key to create tokens is to allow for identification of corresponding patient records, and the tokens stored in Landi’s central processing system correspond to tokens in the query. *Id.* at 58–59 (citing Clark Decl. ¶¶ 216–217). Petitioner further asserts “Landi also describes where tokens would be matched when querying for patient records associated with a clinical trial.” *Id.* at 59–60.

Petitioner provides similar analyses for claim limitations 7[d]–7[k]. Pet. 60–65; Clark Decl. ¶¶ 219–229. We find that for the reasons given, Petitioner has demonstrated a reasonable likelihood of prevailing on this obviousness challenge to claim 7 based on Dick and Landi.

2. Claims 1–6 and 8–19

As noted, Petitioner asserts that claims 8–10 and 13 would have been obvious over Dick and Landi and provides an element-by-element analysis for each of those claims supported by testimony from Dr. Clark. Pet. 65–66; Clark Decl. ¶¶ 230–234. We find that for the reasons given at this stage, Petitioner, supported by testimony from Dr. Clark, has demonstrated a reasonable likelihood of prevailing on these challenges.

Similarly, Petitioner provides an element-by-element analysis for claims 1–6, 11, 12, and 14–19 in relation to Dick, Landi and Murphy. Pet.

67–74; Clark Decl. ¶¶ 243–272. Further, Petitioner provides a motivation to combine the references. Pet. 67–68; Clark Decl. ¶¶ 236–238. We find that for the reasons given, Petitioner has demonstrated a reasonable likelihood of prevailing on these challenges.

III. CONCLUSION

For the foregoing reasons, we have determined that there is a reasonable likelihood that the Petitioner would prevail with respect to at least one of the claims challenged in the Petition. We therefore institute trial as to all challenged claims on all grounds stated in the Petition. 37 C.F.R. § 42.108(a).

IV. ORDER

For the foregoing reasons, it is

ORDERED that pursuant to 35 U.S.C. § 314(a), an *inter partes* review of the '641 patent is hereby instituted for all of the challenged claims on all of the asserted grounds; and

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

IPR2024-00226
Patent 9,118,641 B1

For PETITIONER:

Peter Shapiro
Justin Oliver
Nicholas Marcello
Michael Sandonato
VENABLE LLP
PShapiro@venable.com
JOliver@Venable.com
NDMarcello@venable.com
Datavant-IPRs@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