

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DATAVANT, INC.,
Petitioner,

v.

VIGILYTICS LLC,
Patent Owner.

Case IPR2024-00226
Patent 9,118,641 B2

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I. Introduction.....1

II. Overview of the '641 Patent.....2

 A. Overview of the Technology.....2

 B. HIPAA Background 9

 C. Person of Ordinary Skill in the Art 11

III. Claim Construction 12

IV. Ground 1: Evenhaim Fails to Render the Challenged Claims Obvious 12

 A. Overview of Evenhaim (EX1005).....12

 B. Analysis 15

 1. Evenhaim’s data aggregator does not produce a token for each individual included in a group composed of multiple individuals identified in a request.....16

 2. Evenhaim’s data aggregator does not convey request tokens for individual patients to data source entities 23

 3. Evenhaim’s data source entities do not perform the alleged “token matching” to search de-identified healthcare data 30

V. Ground 2: The Evenhaim-Settimi Combination Fails to Render the Challenged Claims Obvious.....35

 A. Overview of Settimi (EX1006) 35

 B. Analysis 36

 1. The Evenhaim-Settimi combination fails to disclose or render obvious multiple limitations of independent claims 1, 7, and 14 37

 2. The Evenhaim-Settimi combination would not have been obvious because integration of Settimi’s teachings would have

violated Evenhaim’s express preference for searching original,
micro-level patient data.....39

VI. Ground 3: The Dick-Landi Combination Fails to Render the Challenged Claims Obvious.....	41
A. Overview of Dick (EX1007)	41
B. Overview of Landi (EX1008)	44
C. Analysis	47
1. The Petition fails to demonstrate a motivation to combine Dick and Landi.....	48
2. The Dick-Landi combination does not disclose or render obvious elements [1.b]-[1.c], [7.a]-[7.b], or [14.c]-[14.d]: an encryption server for producing a token for individuals in a group identified in a request for healthcare information	53
3. The Dick-Landi combination does not disclose or render obvious elements [1.f], [7.e]-[7.f], [14.f]: identifying tokens in a set of de-identified healthcare data that correspond to request tokens for individuals in a group	59
4. The Dick-Landi combination does not disclose or render obvious elements [1.h], [7.h], [14.h]: the produced healthcare information is absent personally identifiable information.....	62
VII. Ground 4: The Dick-Landi-Murphy Combination Fails to Render the Challenged Claims Obvious.....	64
A. Overview of Murphy (EX1009).....	64
B. Analysis	65
VIII. CONCLUSION	69

EXHIBIT LIST

Exhibit No.	Description
2001	Expert Declaration of Aviel D. Rubin, Ph.D.
2002	Transcript of Deposition of Paul C. Clark, September 26, 2024
2003	Summary of HIPAA Privacy Rules (https://www.hhs.gov/sites/default/files/privacysummary.pdf)
2004	Summary of the HIPAA Security Rule (https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html)
2005	HIPAA History (https://www.hipaajournal.com/hipaa-history/)
2006	45 C.F.R. §164.514 (Other requirements relating to uses and disclosures of protected health information)
2007	45 C.F.R. §75.2 (Definitions)

CLAIM ELEMENT LISTING

Claim 1	
1.a	A computer-implemented method comprising: receiving a request for healthcare information that characterizes a group composed of multiple individuals, the healthcare information being assembled from healthcare data that comprises de-identified information;
1.b	producing, by a processor of an encryption server, tokens,
1.c	wherein the identity of the individuals in the group is unattainable from the tokens, each token being associated with an individual in the group, each token being associated with a corresponding token in a set of de-identified healthcare data, and
1.d	each token in the set of de-identified healthcare data being associated with healthcare data for a corresponding individual;
1.e	when the group includes at least a minimum number of individuals,
1.f	producing the requested healthcare information that characterizes the group 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,
1.g	wherein the produced tokens and the tokens in the set of de-identified data are similarly encrypted, and
1.h	the produced healthcare information is absent personally identifiable information and
1.i	has been produced without the individuals in the group having authorized production of such healthcare information that characterizes the group; and

1.j	providing the produced healthcare information to report the characteristics of the group composed of multiple individuals absent authorization at any time from the individuals in the group of individuals to provide the requested healthcare information.
Claim 2	
2	The computer-implemented method of claim 1, wherein the healthcare information provided absent authorization from the group of individuals at any time is in conformity with the Health Insurance Portability and Accountability Act (HIPAA).
Claim 3	
3	The computer-implemented method of claim 1, wherein receiving a request for healthcare information that characterizes a group of individuals from healthcare data includes receiving personally identifiable information associated with members of the group of individuals.
Claim 4	
4	The computer-implemented method of claim 1, in which producing the requested healthcare information includes encrypting respective data that identifies each individual.
Claim 5	
5	The computer-implemented method of claim 1, in which producing the requested healthcare information includes identifying at least a minimum number of corresponding tokens.
Claim 6	
6	The computer-implemented method of claim 1, in which the healthcare data represents medical related information associated with the

	individuals of the group.
Claim 7	
7.a	A system comprising: an encryption server, having a processor and a memory,
7.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,
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,
7.d	and each token in the set of de-identified healthcare data being associated with healthcare data for a corresponding individual;
7.e	a data server for producing the requested healthcare information that characterizes the group
7.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,
7.g	wherein the produced tokens and the tokens in the set of de-identified data are similarly encrypted,
7.h	and the produced healthcare information is absent personally identifiable information
7.i	and has been produced without the individuals in the group having authorized production of such healthcare information that characterizes the group; and
7.j	providing the produced healthcare information to report the characteristics of the group composed of multiple individuals

7.k	absent authorization at any time from the individuals in the group of individuals to provide the requested healthcare information.
Claim 8	
8	The system of claim 7, wherein the healthcare information provided absent authorization from the group of individuals at any time is in conformity with the Health Insurance Portability and Accountability Act (HIPAA).
Claim 9	
9	The system of claim 7, wherein the request for healthcare information that characterizes a group of individuals from healthcare data includes personally identifiable information associated with members of the group of individuals.
Claim 10	
10	The system of claim 7, in which producing the requested healthcare information includes encrypting respective data that identifies each individual.
Claim 11	
11	The system of claim 7, in which producing the requested healthcare information includes identifying at least a minimum number of corresponding tokens.
Claim 12	
12	The system of claim 7, in which producing the requested healthcare information includes determining if the group includes at least a minimum number of individuals.
Claim 13	
13	The system of claim 7, in which the healthcare data represents medical

	related information associated with the individuals of the group.
Claim 14	
14.a	One or more computer readable storage devices storing instructions that are executable by a processing device, and upon such execution cause the processing device to perform operations comprising:
14.b	receiving a request for healthcare information that characterizes a group composed of multiple individuals, the healthcare information being assembled from healthcare data that comprises de-identified information;
14.c	producing, by a processor of an encryption server, tokens,
14.d	wherein the identity of the individuals in the group is unattainable from the tokens, each token being associated with an individual in the group, each token being associated with a corresponding token in a set of de-identified healthcare data, and each token in the set of de-identified healthcare data being associated with healthcare data for a corresponding individual;
14.e	when the group includes at least a minimum number of individuals,
14.f	producing the requested healthcare information that characterizes the group 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,
14.g	wherein the produced tokens and the tokens in the set of de-identified data are similarly encrypted, and
14.h	the produced healthcare information is absent personally identifiable information and has been produced without the individuals in the group having authorized production of such healthcare information that

	characterizes the group; and
14.i	providing the produced healthcare information to report the characteristics of the group composed of multiple individuals absent authorization at any time from the individuals in the group of individuals to provide the requested healthcare information.
Claim 15	
15	The computer readable storage devices of claim 14, wherein the healthcare information provided absent authorization from the group of individuals at any time is in conformity with the Health Insurance Portability and Accountability Act (HIPAA).
Claim 16	
16	The computer readable storage devices of claim 14, wherein the request for healthcare information that characterizes a group of individuals from healthcare data includes personally identifiable information associated with members of the group of individuals.
Claim 17	
17	The computer readable storage devices of claim 14, in which producing the requested healthcare information includes encrypting respective data that identifies each individual.
Claim 18	
18	The computer readable storage devices of claim 14, in which producing the requested healthcare information includes identifying at least a minimum number of corresponding tokens.
Claim 19	
19	The computer readable storage devices of claim 14, in which the healthcare data represents medical related information associated with

	the individuals of the group.
--	-------------------------------

I. INTRODUCTION

Vigilytics LLC (“Patent Owner”) submits this Patent Owner’s Response (“POR”) in IPR2024-00226, in which Datavant, Inc. (“Petitioner”) challenges the patentability of claims 1–19 (the “Challenged Claims”) of U.S. Patent 9,118,641 (“’641 patent”; EX1001). As explained below, Petitioner fails to establish by a preponderance of the evidence that the claims are unpatentable.

In Ground 1, the Petition mischaracterizes key aspects of Evenhaim’s disclosure. Among other things, the Petition conflates Evenhaim’s separate encryptions for data transmission security and data mergers to conjure an embodiment in which data source entities allegedly search de-identified patient data by matching encrypted request tokens to corresponding tokens associated with the de-identified data. But these features are never disclosed in Evenhaim and Evenhaim’s system would never operate as Petitioner contends. The Petition’s interpretation of Evenhaim is both contradicted by portions of the reference not acknowledged in the Petition and is inconsistent with Evenhaim’s express teaching against searching on de-identified or agglomerated data, as would be required by Petitioner’s theory. Ground 2 based on Evenhaim in view of Settimi suffers from these same defects as Ground 1, along with additional problems as described herein.

Grounds 3 and 4 fare no better. In Ground 3, the Petition fails to

demonstrate a motivation to combine Dick and Landi. Even if combined, the resulting system would not achieve multiple limitations recited in the Challenged Claims. The combination, for example, would entirely lack an encryption server that produces a token for each individual included in a group composed of multiple individuals identified in a request for healthcare information.

Ground 4 adds Murphy to the Dick-Landi combination but inherits the same defects from Ground 3. The Petition’s reliance on Murphy is also non-availing as Murphy does not block queries as assumed in the Petition.

For each of these and the additional reasons described in detail in this Response, the Petition fails to show that any of the Challenged Claims would have been obvious. Grounds 1–4 should accordingly be dismissed and the patentability of the claims confirmed.

II. OVERVIEW OF THE ’641 PATENT

A. Overview of the Technology

The ’641 Patent explains that health insurers previously lacked sufficient access to protected health information (“PHI”) stored by health providers, such as pharmacies, for individuals in small and midsize groups (e.g., groups of 10–1000 individuals). EX1001, 1:14–36; EX2001, 56–63. PHI for members in these groups, such as an individual, e.g., “Jack,” and his dependents, could be used by health insurers to better understand, assess the risk, and appropriately price

premiums for the associated future cost of providing health insurance to the group.

EX1001, 4:4–24. The PHI for Jack was previously insufficiently accessible

because, as the '641 Patent explains, Federal laws, such as the Health Insurance

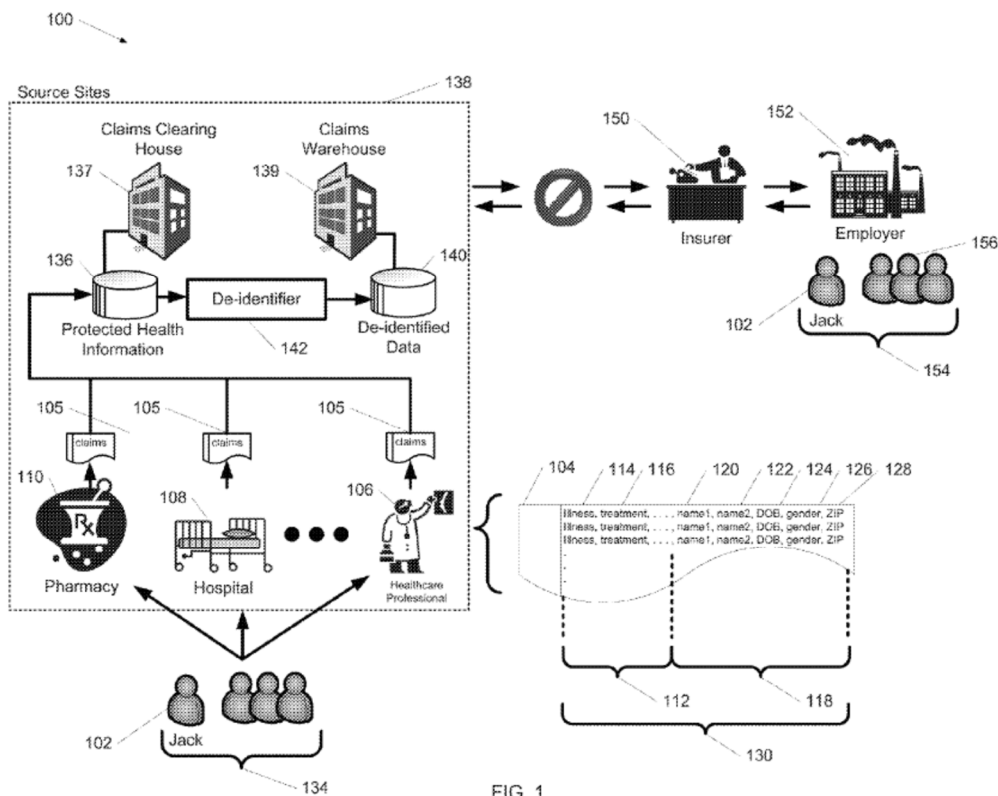
Portability and Accountability Act (“HIPAA”), prohibit source sites that possess

Jack’s PHI from releasing it to third parties without Jack’s permission. Under

HIPAA, the source sites can release only irreversibly de-identified data without

Jack’s (or another patient’s) permission. EX1001, 3:65–4:3. PHI can include

“[d]ata that associates patient identity with health information” *Id.* at 1:26–28.



'641 Patent, FIG. 1

As shown in FIG. 1 above, a “health insurer 150, for example, may be

interested in the medical history information contained in Jack's PHI 130. Jack's employer 152 may like to buy a group health insurance policy for the group 154 made up of Jack 102 and his coworkers 156. If the group 154 is too small, the insurance company 150 may be unwilling or unable to share medical claims history with the group 154 that would allow for an assessment of the potential risk from future medical claims for the group 154." EX1001, 4:4–24.

When the history or experience is not available for small groups, insurers before the present invention generally could only rely on less informative data such as age and gender to rate the groups and set a group insurance premium. As a result, the insurer is left with an incomplete understanding of the risk of the group and a hesitancy to seek out the business. The result for the small and mid-sized groups is less choice since insurers are not willing to take on the risk. More, the de-identified data, which the healthcare providers or other source sites could release without permission, is not useful to the insurer because the insurer has no way to know whether it corresponds to the people in a given group.

To address these problems, the '641 Patent discloses novel methods and systems to implement specific token generation and anonymization approaches to achieve a new computer capability: systems able, in response to a request for information regarding a group of individuals who have not authorized PHI disclosure, to provide to third parties (e.g., insurance companies or professional

employer organizations, known as “PEOs”) irreversibly de-identified healthcare information from which the third party may calculate a risk score used in setting an insurance premium for the group, while complying with federal privacy regulations, including HIPAA.¹ *See, e.g., id.*, 4:25–30. This was a significant advancement because prior to the invention, signed authorizations had to be collected from individuals in the request, which was an impediment to a viable product. Although tokenized health data had been used for other purposes prior to the ’641 Patent, it had not been used in the particular context or manner described in the ’641 Patent. *Id.* FIG.3 illustrates an example system implemented in accordance with the novel solutions described in the ’641 Patent:

¹ Notably, the irreversibly de-identified healthcare information for individuals is released to a third party that does not have access to the personally identifying information (PII) used to generate the request. This prevents the third-party might from matching PII from the request to the de-identified data patient-level data to uncover the patient’s identify. EX2001, 56–63.

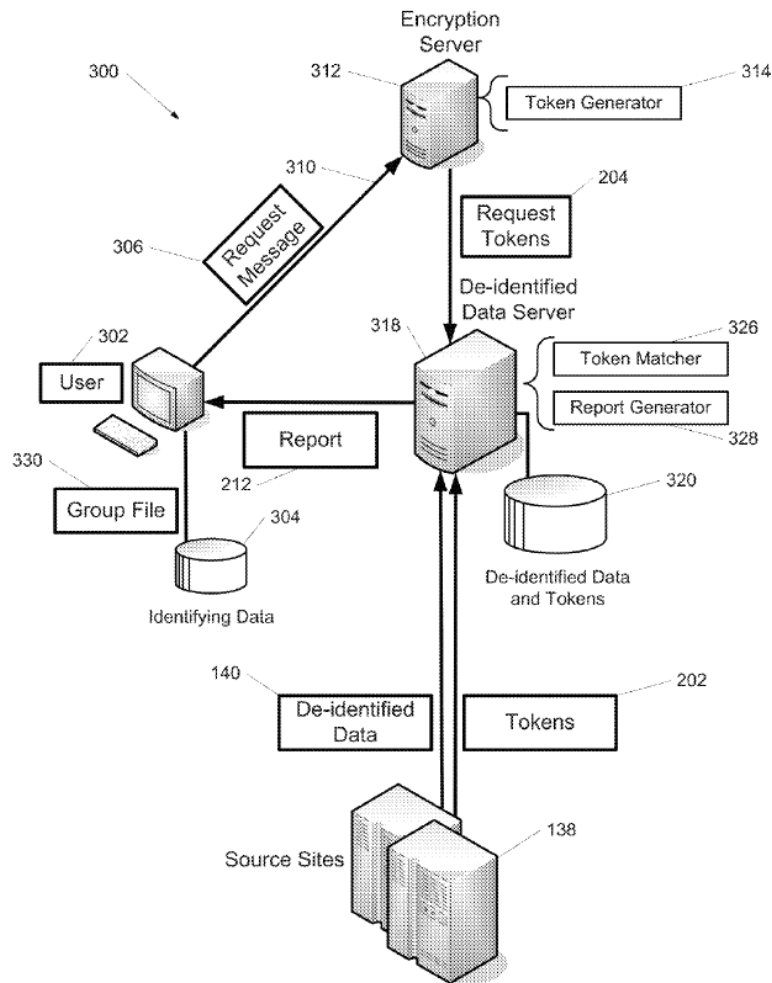


FIG. 3

As shown in FIG. 3, a user, e.g., an insurer, requests de-identified data that characterizes a group of identified individuals, where the de-identified data may reflect information regarding medical claims, hospital claims, and prescription history (such as the drug categories and drug indications associated with the drugs in the de-identified data). EX1001, 6:6–8, 6:59–62. In this example, the insurer can send a request to a third party. *Id.*, 4:32–33. The request “uniquely identifies” each individual in the group, which could be a group of individuals for

which health insurance is sought. *Id.*, 5:12–30. The third party, for example using an “encryption server,” generates a “request token” for each individual in the group based on the personally identifiable information for each individual in the group. *Id.*, 4:32–35, 5:35–38. The encryption server can generate the request token such that the request token is similarly encrypted to the token associated with the information to be produced. *Id.*, 2:16–18. For example, the encryption server may use the same token generator as used to generate the tokens for the de-identified data or it may use any other means that generates a comparable token for the same personally identifiable information. *Id.*, 5:44–67.

The identities of the individuals are unattainable from the tokens implemented according to the '641 Patent. *Id.*, 4:30–32. That way, the tokens are reproducibly irreversible. *Id.*, 4:29–30 (system “associates unique tokens 202 with irreversibly de-identified data 140”), 6:8–12 (the de-identified data is processed “in a way that leaves it irreversibly de-identified”). In that connection, the tokens are generated from personally identifiable information of the individuals using “one or more encryption techniques” such as a hash function. *Id.*, 5:54–67.

In one configuration, the encryption server sends generated request tokens to the data aggregator, or de-identified data server, that stores the de-identified healthcare data. *Id.*, 4:35–37, 5:44–49. The data aggregator (or de-identified data

server) stores irreversibly de-identified healthcare data for many individuals. The de-identified healthcare data can comprise data from source sites such as pharmacies, healthcare professionals and electronic claim clearing houses. *Id.*, 5:45–49. The tokens are associated with the de-identified healthcare data of individuals. The data server, with a token matcher, can find all tokens in the de-identified healthcare data that match the request tokens from the encryption server. *Id.*, 4:37–41, 6:1–4. The de-identified healthcare data for the matched tokens can then be processed in a way that leaves it irreversibly de-identified, yet useful for an underwriting assessment of the group. *Id.*, 4:37–45, 6:8–15. The aggregator can retrieve the requested de-identified data for each of the individuals in the group, and the aggregator can provide the de-identified data associated with the group of individuals, without revealing the protected health information of the individuals in the group and without obtaining any authorization from the individual members of the group. This de-identified data can be included in a report provided to the user after tokens in the request are matched to tokens in the de-identified data. *Id.*, 6:62–67, 8:17–27, 8:27–31, 8:41–43. The recipient of the report, e.g., the insurer which has personally identifiable information about the individuals in the group does not have access to data associated with specific individuals. *Id.*, 4:51–54. “These features of the system maintain the privacy of the protected health information.” *Id.*, 4:59–61 (reference numbers omitted).

The '641 Patent explains that the above-described process may not be performed unless the request includes a minimum number of individuals. The minimum number (e.g., 10) is “chosen to make it effectively impossible to associate individual group members with individual tokens in the batch of request tokens” *Id.*, 5:40–43, FIGS. 2–3, 5–6.

B. HIPAA Background

As noted above, the technology described and claimed in the '641 Patent allows entities such as insurance carriers to obtain reports that characterize de-identified health care data for a specific group of individuals while still complying with patient privacy laws such as HIPAA. *Supra*, §II.A. While the inventive technology is not limited to systems and methods that operate within the constraints of HIPAA, HIPAA nonetheless features prominently in examples described in the specification of the '641 Patent, the Petition's asserted prior art, and the obviousness analyses of the Petitioner and its witness (Dr. Clark). Particular aspects of HIPAA relevant to the parties' dispute are reviewed below. EX2001, 64.

The HIPAA “Privacy Rule” is a rule issued by the Department of Health and Human Services (HHS) under HIPAA. The Privacy Rule “address[es] the use and disclosure of individuals' health information—called ‘*protected health information*’ [or PHI] by ‘*covered entities*’—or organizations that are subject to

the Privacy Rule,” as well as standards for individuals’ privacy rights to

understand and control how their health information is used.² EX2003, 3³.

While not expressly using the term “HIPAA Privacy Rule,” the ’641 Patent refers to it. For example, the ’641 Patent explains that “Federal privacy laws . . . prevent insurance companies from obtaining protected health information without individual authorizations from [] each person in the group” and that HIPAA prohibits source sites that process a person’s PHI from releasing to third parties the person’s PHI without the person’s permission. EX1001, 1:33–36, 3:65–4:2.

The ’641 Patent also explains, consistent with the HIPAA Privacy Rule, that source sites that process a person’s PHI can release only irreversible deidentified without the person’s permission. EX1001, 4:2–3; EX2003, 3; EX1008, 2:5–18; EX1005, 2:5–57. This is part of how the systems described in the ’641 Patent comply with HIPAA, by using de-identified healthcare data so that authorizations from the individuals in a request group are not required. EX2001, 65–68.

Notably, not all organizations are covered entities who must comply with

² All emphasis added unless indicated otherwise.

³ All citations to page numbers are to the marked page number of the exhibit PDF unless indicated otherwise.

the HIPAA Privacy Rule. An entity that does not process or have access to PHI may nonetheless possess personally identifying information (PII) about individuals (e.g., names, phone numbers, and the like). It would not violate HIPAA for such entities to use the individuals' PII to request healthcare information about a group of individuals. EX2001, 65–68; EX2003–EX2007; *see also* EX2004, 2; EX2004, 5–10, EX2001, 69–70 (describing HIPAA “Security Rule” for electronic PHI (ePHI)).

C. Person of Ordinary Skill in the Art

The Petition contends that a person of ordinary skill in the art (“POSITA” or “POSA”) “would have 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 EX1003, ¶22).

Patent Owner agrees that a POSITA would possess the educational and professional experiences described in the Petition, although these experiences alone do not fully capture the minimum qualifications of a POSITA in the field of the '641 Patent. EX2001, 71–72. A POSITA would also have familiarity with medical records and databases for storing medical records—particularly in manner that complies with privacy laws and regulations such as HIPAA. *Id.* The '641 Patent was solving a computer science problem in the abstract, but was instead

solving such a problem in the context of privacy laws and regulations that would ordinarily prevent entities from analyzing medical data associated with a specific group of individuals. *Id.* Familiarity with medical records systems and their design for compliance with applicable privacy laws and regulations would have been fundamental to the knowledge and skill of a POSITA of the '641 Patent. *Id.*

III. CLAIM CONSTRUCTION

Claims in an IPR are interpreted under the *Phillips* standard. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100.

Because this Response addresses deficiencies in the Petition's analysis that do not appear to turn on disputed claim scope, Patent Owner does not formally construe any claim terms at this time. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011) ("claim terms need only be construed to the extent necessary to resolve the controversy.") (internal citations omitted); EX2001, 73–74. Patent Owner reserves all rights to address claim constructions later raised by the Petitioner or the Board.

IV. GROUND 1: EVENHAIM FAILS TO RENDER THE CHALLENGED CLAIMS OBVIOUS

A. Overview of Evenhaim (EX1005)

Evenhaim discloses a system that allows for searching of PHI at source entities such as pharmacies or healthcare providers. EX1005, 1:14–19, Abstract. Unlike the '641 Patent, Evenhaim relies on the source entities to search PHI

directly and to de-identify patient-level data only after they are searched.

EX1005, 6:15–25, 17:43–52; EX2001, 76–79.

For example, Evenhaim’s system includes an aggregator processor connected to one or more source-entity processors, each source-entity processor corresponding to an organization that maintains PHI for individuals. EX1005, 5:12–28, FIGS. 4, 4A. The aggregator processor receives queries from consumer-entity processors, and from the queries, generates search requests for the source-entity processors. EX1005, 6:56–67, 7:1–27. The source-entity processors search their original micro-level data—including patients’ PHI—to identify records responsive to the search request. EX1005, 6:15–25, 17:43–52. Once patient level data has been identified responsive to the requests, the source-entity processors de-identify those records and return them in “files” to the aggregator processor. EX1005, 7:20–24. The aggregator processor aggregates files received from each of multiple source-entity processors and reports an agglomerated extract of the files to the consumer-entity in response to the query. EX1005, 9:13–27.

Notably, the search request sent from the aggregator processor to each of the source-entity processors can include a parameter list that carries “privacy sensitive micro-data” such as the names or IDs of individuals (e.g., patients) who are the subject of the request. EX1005, 8:30–48. However, Evenhaim never produces tokens from the patient names in the search request, and Evenhaim’s

source-entity processors never match any such tokens to de-identified data

records. Evenhaim thus fails to disclose, among other things, an unauthorized

party using an encryption server to query a database for de-identified healthcare

information concerning a group of known individuals or a data server producing

requested healthcare information that characterizes the group. EX2001, 76–79.

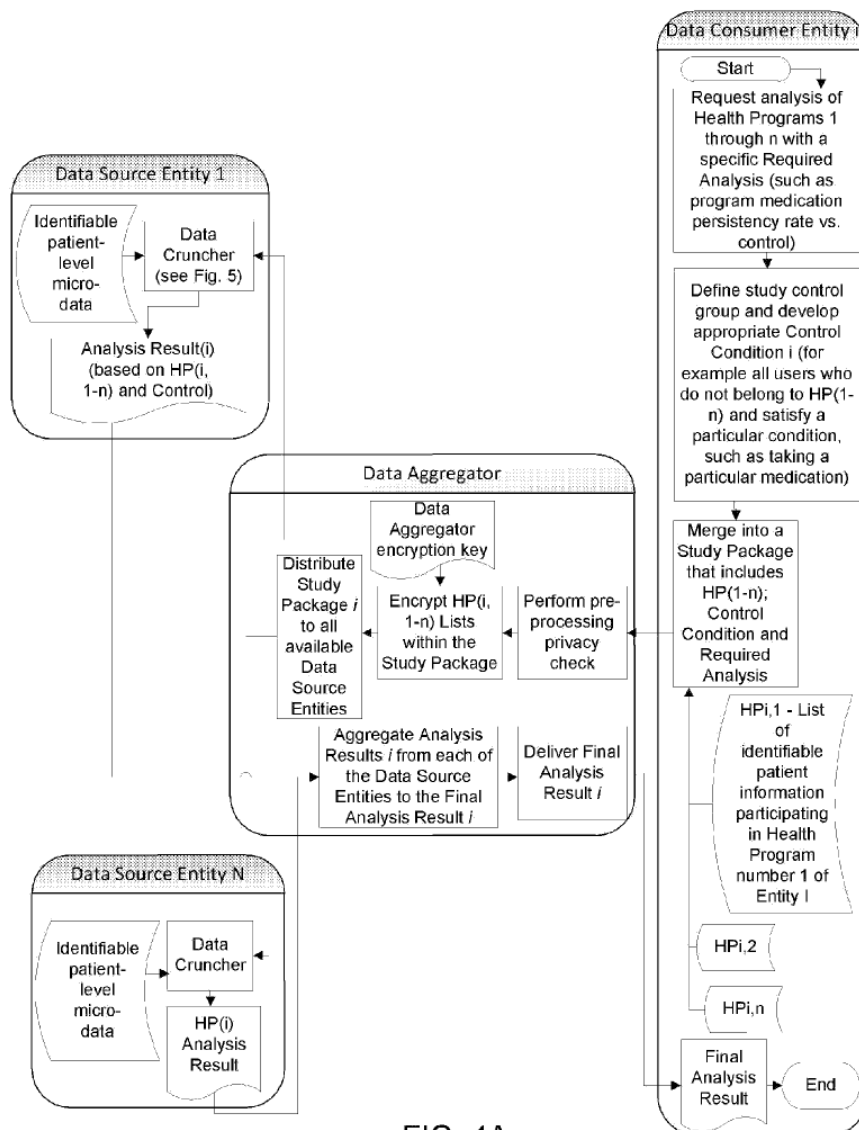


FIG. 4A

Evenhaim, FIG. 4A

B. Analysis

The Petition relies on a distorted interpretation of Evenhaim that mischaracterizes the reference's express teachings, and indeed, fundamentally alters the system Evenhaim expressly describes. EX2001, 100–137. Whether borne of a mistaken understanding of Evenhaim's disclosure or a flawed attempt to stretch its disclosure onto the Challenged Claims, the Petition's use of Evenhaim reveals impermissible hindsight and should be rejected. *In re Fritch*, 972 F.2d 1260, 1266 (Fed. Cir. 1992) (“It is impermissible to use the claimed invention as an instruction manual or ‘template’ to piece together the teachings of the prior art so that the claimed invention is rendered obvious.”) (citations omitted).

The overarching problem in the Petition's application of Evenhaim is that the Petition wrongly assumes Evenhaim discloses an embodiment where the data source entities search de-identified patient records by matching tokens received from the data aggregator with corresponding tokens in a database of de-identified medical records. EX1003, ¶39. But Evenhaim never discloses nor suggests such an embodiment. EX2001, 100–137. This embodiment is instead invented entirely by Petitioner and its witness, Dr. Clark, with the '641 claims themselves being the only apparent basis from which this embodiment was injected in Evenhaim.

Petitioner’s mischaracterization of Evenhaim involves at least three flawed premises, each of which is addressed in further detail below. *See* EX1005, 14:60–63; EX2001, 100–137.

1. Evenhaim’s data aggregator does not produce a token for each individual included in a group composed of multiple individuals identified in a request

To start, the Petition’s assertion that Evenhaim’s data aggregator produces tokens for individual patients is false. EX2001, 100–137. Petitioner and Dr. Clark cite and conflate two distinct contexts in which Evenhaim’s data aggregator performs encryption—namely, (1) encryption for data transmission security and (2) encryption for data mergers—but neither involves creating tokens for individual patients as alleged. *Id.*

In the first context, Evenhaim provides encryption for data transmission security between the data aggregator and other entities. Evenhaim explains that “it is generally preferable to include some degree of *data transmission security*” by performing “encryption and decryption” for “every step requiring a *transmitting* of data (or of at least one file) and every respective associated step requiring *receiving* of that data (or of that at least one file).” EX1005, 13:33–41; EX2002, 37:23–38:15, 44:2–10.

Evenhaim’s data transmission security scheme involves encrypting the “patient list and query” that the data aggregator transmits to the data source

entities. EX2001, 100–137. This is illustrated in FIG. 4, for example, which shows a single “data aggregator encryption key” being applied to encrypt the patient list and query, thereby ensuring that the contents of the patient list and query will not be revealed to unauthorized actors during transmission, or revealed until the intended data source entity performs an authorized decryption. *Id.* But Evenhaim’s data transmission encryption does not involve token production for requested individuals as claimed. Indeed, during his deposition, Dr. Clark himself agreed that Evenhaim supports the interpretation that the patient lists are encrypted to provide data transmission security (EX2002, 43:2–10):

2	Q. Is it possible that the patient list is
3	encrypted to provide data transmission security in
4	Evenhaim?
5	A. Anything is possible. I mean, that's why
6	Evenhaim has so much disclosure.
7	Q. There is nothing that contradicts that
8	understanding in Evenhaim?
9	A. There's -- no, there's certainly -- at least
10	one of the embodiments would function that way.

Encrypting entire patient lists (and query), as disclosed in Evenhaim, is far different from producing a token for each patient named in the list, which would be inefficient and unnecessary for data transmission security in any event.

EX2001, 100–137. Evenhaim is clear that only the patient lists, and not identifiers for each individual in the list, are encrypted at the data aggregator, thus permitting the data source entities to decrypt the lists with an appropriate decryption key.

See, e.g., EX1005, 14:3–7 (“***Returning to the abovementioned aspects of preferable encryption***, it is certainly strongly advised that regardless of the general level of encryption elected, ***a parameter list including ‘individuals’*** should carry a stronger level of ***encryption.***”), 15:61–65 (“***Encrypting the lists*** using any industry grade encryption method; and Delivering the lists of participants together to a query engine with a capability to ***decrypt the lists*** at the time of processing ...”), FIG. 5 (showing decryption of each “patient identifier ***list***”); EX2001, 100–137.

Notwithstanding Evenhaim’s seemingly clear disclosure, Petitioner argues that the data aggregator “encrypts the names, which a POSA would understand involves ***creating an encrypted token for each individual.***” Pet., 13. The only evidence cited in support of this assertion is the uncorroborated and conclusory declaration testimony of Dr. Clark—which never once acknowledges Evenhaim’s concern with data transmission security or explains how encrypting patient ***lists*** would include producing tokens for ***individual*** patients (it does not). *Id.* (citing EX1003, ¶¶41, 44–45). Although Dr. Clark admits during deposition that the encryption of the patient list could be merely for the purpose of providing data

transmission security, neither his declaration nor the Petition makes any attempt to explain why a POSA would abandon such a common-sense read of Evenhaim—which would be supported by the intrinsic disclosure of the reference—to adopt the convoluted token production and matching theory that finds no support within the four corners of the reference.

Neither Petitioner nor Dr. Clark can square their assertion with the words of the reference itself, which describes encrypting the patient *list* and query, rather than producing tokens for individual patients. Nor can the Petition or Dr. Clark support their contention that any alleged tokens resulting from encryption of the patient list would be compared to corresponding tokens for de-identified patient data at the source entities. *Id.* This theory assumes that alleged tokens from the patient list would not be decrypted by the data source entities since those tokens would be compared to corresponding tokens, but Evenhaim explicitly teaches the contrary: “every step requiring a transmitting of data ... and every respective associated step requiring receiving of that data ... may preferably include respective encryption *and decryption.*” EX1005, 13:33–36, FIG. 5; EX2001, 100–137.

The Petition’s and Dr. Clark’s additional citations to Evenhaim’s “interim data merger enabled embodiments” are similarly unavailing and fail to show that the data aggregator ever generates encrypted tokens for individuals identified in a

request that would be sent in a query to any data source entity. EX1003, ¶39; EX1005, 12:4–13:20. As an initial matter, Evenhaim’s “interim data merger enabled embodiments” involve encryption in an entirely different context from encrypting the patient list and query for data transmission security, as described elsewhere in Evenhaim. EX2001, 100–137. Indeed, as noted above, the patient lists encrypted at the data aggregator for data transmission security are *decrypted* by the data source entities, while the data merger enabled embodiments discussed in column 12 of Evenhaim specifically cautions that the party receiving the encrypted data should *not* be capable of decrypting that data. *Compare* EX1005, 13:33–35 (“every step requiring a transmitting of data ... preferably include[s] respective encryption *and decryption*”) and 15:63 (“decrypt the *lists*”) *with* 12:16–20 (“special care must be taken that the entity performing the linkage is *not capable of knowing the key and decryption function*; because knowing these facets would enable a breach of the individual’s privacy”); EX2001, 100–137. It would be non-sensical for the data source not to decrypt a patient list and query that the aggregator has encrypted for data transmission security. *Id.* The notion that decrypting patient lists at the source entity would implicate a breach of privacy of the type described at 12:16–20 is similarly non-sensical, especially as the patient list contains no PHI and Evenhaim expressly discloses embodiments where such decryption is performed without breaching patient privacy. *See, e.g.,*

EX1005, FIG. 5 (“Decrypt patient identifier list”). Petitioner’s and Dr. Clark’s arguments ignore these facts and repeatedly conflate encryption for data transmission security with the encryption described at column 12 of Evenhaim.

To be clear, Evenhaim never once discloses or suggests that its “interim data merger embodiments” would involve the data aggregator producing tokens for individual patients that would be shared with the data source entities as alleged. EX2001, 100–137. Dr. Clark repeatedly cites Evenhaim’s statement that “the encryption of individual identification and/or merger of data for individuals could be facilitated ... on the ‘aggregator’ processor side” (*see* EX1005, 12:24–29), but this one line is far too vague to support anything like the detailed scheme that Petitioner and Dr. Clark attempt to inject into Evenhaim as part of their mapping to the ’641 claims. EX2001, 100–137; EX2002, 46:25–47:6, 47:8–19. If anything, this one line would suggest something entirely different from what Petitioner and Dr. Clark claim in any event. For example, Evenhaim only specifically discloses “encryption and/or merger” on the data aggregator occurring during the steps of “receiving a respective file, or aggregating the plurality of files,” while conspicuously omitting any mention of the aggregator encrypting the identities of each patient in the patient list itself. EX1005, 12:30–32. The steps of “receiving a respective file, or aggregating the plurality of files” notably occur

upon the aggregator's receipt of *response(s)* to the queries and are not at all related to encrypting the query itself. *See id.*, 7:3–6, FIG. 3.

Producing tokens for individual patients at the data aggregator to query the data source entities is also non-sensical because it would require the data source entities to take inefficient steps of either (i) decrypting the tokens before searching for the appropriate patients' data records or (ii) pre-generating corresponding tokens for patient data records that could be compared against the tokens received from the data aggregator. EX2001, 100–137. Considering the significance of these steps, one would reasonably expect Evenhaim to describe them, or even mention them at all, if the interim-data merger enabled embodiments were intended to cover Petitioner's interpretation. But Evenhaim is entirely silent in this regard. Worse, the embodiment invented in the Petition would itself risk a HIPAA violation if the data source entities released de-identified patient data to the data aggregator that included the patient's token, as would occur to permit linking of data records at the aggregator. EX1005, 12:53–13:20; EX2001, 100–137; EX2002, 47:8–19, 53:12–22. In this case, the data aggregator would be capable of comparing the token it received from the source entity to the token it earlier sent in the queries, thereby permitting the aggregator to correlate the patient's name or other identifier from the patient list to de-identified patient level data released from the source entities in violation of the patient's privacy and

regulations such as the HIPAA Privacy Rule. *Id.* These and other concerns are described in further detail below.

2. Evenhaim’s data aggregator does not convey request tokens for individual patients to data source entities

Even if Petitioner’s assertion that Evenhaim generates individualized tokens for each patient in the patient list were taken at face value (which it does not), Evenhaim does not disclose, and it still would not have been obvious, to query the data source entities with those tokens in Evenhaim’s system. EX2001, 100–137.

For context, Petitioner’s witness, Dr. Clark, contends that Evenhaim “produce[s] encrypted tokens *that are distributed as a query to the data sources.*” EX1003, ¶40. Dr. Clark appears to infer this position solely from Evenhaim’s disclosure that “[t]here are numerous locations where an encryption of individual identification ... could be facilitated,” including on the ‘aggregator’ processor side.” EX1005, 12:24–34. But this terse disclosure does not support Dr. Clark’s position. Nowhere does Evenhaim imply that the output of such encryption is either (i) distributed to the data sources or (ii) used in token matching at the data sources. EX2001, 100–137. Indeed, such distribution of individually encrypted tokens from the aggregator to the data sources would be absurd in the context of Evenhaim’s system for multiple reasons. *Id.*

First, no need exists for the data aggregator to provide the data sources with tokens produced by individually encrypting the patient names or IDs rather than

simply providing the patient names or IDs themselves. *Id.* The patient list and query do not include protected health information (PHI) that would ordinarily dictate a need for de-identification under applicable privacy laws such as HIPAA at least because the names do not originate with a covered entity and they are not obtained from patients' private medical information. *Id.*; EX2002, 49:24–50:5, 57:16–25, 60:12–23. They are simply names or IDs of individuals whose de-identified medical data is requested. EX1005, 7:8:4–5 (“Intrinsically, in the context of the instant invention, the parameters of the list may include identity disclosing specifics”), 8:10–48. By contrast, the data source entities are the entities that originate and maintain PHI in Evenhaim. EX1005, 5:12–28. Data source entities are “organizations that generate, capture, or store (for example, in the health care industry) medical and claims data that includes identifiable personal health information.” *Id.* Data source entities include physician offices, hospitals, labs, pharmacies, and other “Covered Entities” as defined under HIPAA. *Id.*, 5:15–19. As the originators and maintainers of PHI, these entities already know the patients' names and PHI. Requiring the data aggregator to replace patient names with tokens in the request would be nonsensical. EX2001, 100–137. Indeed, any attempts to conceal the patient names from the data source entities would be futile, as the data sources already possess this information. *Id.*

To this point, Dr. Clark’s statements that “the query sent from the aggregator to the data sources should not include personally identifying information” and “transmitting personally identifying information to the data source as part of the query could itself be a potential HIPAA violation” is patently false. EX1003, ¶40. As noted above, the data source entities themselves are “covered entities” under HIPAA (EX1005, 5:12–19), and there can be no HIPAA violation in transmitting a query that contains no PHI to the data sources. EX2001, 100–137.

More, and ironically, it is Petitioner’s invented embodiment that is nowhere disclosed in Evenhaim that actually raises the specter of a HIPAA violation. Under Petitioner’s theory, the data aggregator would both (i) produce tokens from a patient list and (ii) receive matched tokens from the data source entities, thereby rendering the data aggregator capable of recovering patient identities by correlating patient names with returned records from the data source entities without authorization. *Id.* Yet Evenhaim itself warns that the data aggregator or Crossix protocol operator should not be provided medical data from which the identities of individuals could be reasonably derived: “[w]hen releasing data from the data source to the data aggregator, ***the personal IDs will be encrypted—but using the same key*** in all data sources—***a key that will preferably not be known to the Crossix protocol operator...***.” EX1005, 12:61–66; *see also, id.*, 12:16–20

(“special care must be taken that the entity performing the linkage is not capable of knowing the key and decryption function; because knowing these facets would enable a breach of the individual’s privacy”). HIPAA’s de-identification standard specifically states that de-identification must be accomplished such that there “is no reasonable basis to believe that the information can be used to identify an individual.” EX1005, 2:10–12; 45 C.F.R. §164.514(a). But Petitioner’s and Dr. Clark’s proposal to return matched tokens with de-identified health data to the same entity—i.e., the data aggregator—that creates the request tokens in the first place makes it almost certain that the data aggregator could identify individuals and their corresponding healthcare data. Pet., 21, 24; EX1003, 40; EX2001, 100–137. This example also highlights the unreliability of Dr. Clark’s opinions that are underpinned by significant misunderstandings of HIPAA and privacy concerns in general. In this context, and further considering his lack of citations to third-party corroborating evidence or other authority, Dr. Clark’s opinions are entitled to little or no weight. Fed. R. Evid. 702(b); 37 C.F.R. §42.65(a).

Evenhaim’s data aggregator also would not convey request tokens to the data source entities because the data source entities are configured to search original micro-level patient data from which patient names or IDs in the request can be matched against patient names or IDs in the data source entities’ original data records. EX1005, 6:15–34, 9:47–51, 17:41–52; EX2001, 100–137. There is

no token matching at the data source entities in Evenhaim not only because it is unnecessary, but also because it would be contrary to Evenhaim’s specific goal of searching original micro-level patient data ***before it is de-identified or aggregated***. *Id.*; see also EX1005, 17:47–48 (“This analysis is performed on the original, most complete data set”). In fact, any encryption of individually identifying information to produce tokens is only performed by the data sources ***after the relevant data records have already been identified*** for release to the data aggregator and not for the purpose of matching to identify patient data records as alleged: “[A]t substantially each data source there is performed [sic] ***a name matching to identify all of the records*** for a certain identity (e.g. for Jane Doe). ... ***When releasing data from the data source to the data aggregator, the personal IDs will be encrypted***-but using the same key in all data sources-a key that will preferably not be known to the Crossix protocol operator, but only a trusted third party such as an escrow agent.” EX1005, 12:53–66; EX2002, 51:8–17 (“that’s sort of the point of the reference, right?”). Evenhaim thus teaches away from the exact approach that Petitioner and Dr. Clark improperly seek to inject in Evenhaim’s system to force a read on the Challenged Claims of the ’641 Patent. *Galderma Labs., L.P. v. Tolmar, Inc.*, 737 F.3d 731, 738 (Fed. Cir. 2013) (a reference teaches away “when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference,

or would be led in a direction divergent from the path that was taken”); *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1069 (Fed. Cir. 2018) (a primary reference’s “statements regarding preferences are relevant to a finding regarding whether a skilled artisan would be motivated to combine that reference with another reference”); *Plas-Pak Indus. v. Sulzer Mixpac AG*, 600 Fed. Appx. 755, 758–759 (Fed. Cir. 2015) (a change that “fundamentally alters” a reference’s “principle of operation ... is unlikely to motivate a person of ordinary skill to pursue a combination with that reference”); *In re Ratti*, 270 F.2d 810, 813 (CCPA 1959) (declining to find obviousness where the “combination of references would require a substantial reconfiguration and redesign of the elements shown in [the reference] as well as a change in the basic principles under which the [reference's] construction was designed to operate”); *Apple Inc. v. Papst Licensing GMBH & Co. KG*, IPR2016-01842, Paper 35, 39 and 53 (no obviousness where petitioner’s proposed modification would “change[] the principle of operation” of the prior art system).

Evenhaim also specifically illustrates in FIG. 5 a data cruncher module of a data source entity that decrypts a patient identifier list for the very purpose of allowing names from the lists to be matched against names in the original data records. EX1005, Fig. 5; EX2001, 100–137. In fact, name matching or matching based on similar individually identifying information is the only approach

described in Evenhaim for processing the queries received at the data source entities. *See* EX1005, 9:47–51 (“If the parameter list included specific individuals by name or ID or the likes, “Crunching together” may involve ***name matching through “fuzzy logic” and other name matching algorithms of the population*** defined by the parameter list with the source-entity database names, in addition to the other steps defined above.”). By contrast, Evenhaim describes no embodiment where Petitioner’s proposed “token matching” occurs at the data source entities. This again is not surprising, as Evenhaim specifically sought to have the data source entities respond to queries based on analysis of ***raw data*** in its original, most detailed form. EX1005, 6:16–17 (“the instant invention allow[s] analysis of ‘source-entity’ raw data at is original, most detailed form (high resolution data) including full access to all of the privacy sensitive data currently at its disposal . . .”). Evenhaim distinguishes its proposed invention from prior approaches by specifically calling for de-identification to occur ***after name-matching and analysis have been completed on the raw data:***

The instant ***Crossix “method” is based on an opposite sequence: (A) Analyze***-the healthcare organization (such as health plan) runs an analysis software that receive as an input the required analysis and aggregation level as well as possibly ***a list of identifiable patients or physicians for which analysis*** is requested. This analysis is performed on the original, most complete data set; ***(B) De-identify &Aggregate-Once name matching and analysis is complete data is aggregated***

and, if needed, de-identified; (C) and Collect from various sources -Analysis responses from multiple organization are composed to deliver the analyses requested.

EX1005, 17:42–52.

For at least these reasons, Evenhaim fails to even suggest, let alone describe that any tokens produced by the aggregator are distributed as a query to the data sources.

3. Evenhaim’s data source entities do not perform the alleged “token matching” to search de-identified healthcare data

The Petition cites Dr. Clark’s declaration testimony that “[t]here is an embodiment [in Evenhaim] that does not require tokens, but Evenhaim also describes using a token matching system to allow for querying de-identified patient records.” EX1003, ¶19. But this is wrong; the latter embodiment simply does not exist. EX2001, 100–137.

The portion of Evenhaim (12:36–42) that Dr. Clark refers to for this assertion does disclose two embodiments, but not as Dr. Clark characterized them. Evenhaim in fact discloses “two different situations where data *from the data source* is returned already aggregated, after analysis as well as a second option where data is released at the micro-level (each person’s data), but the person identity information, for the matched population, is replaced with a unique encryption key, such as a hash or Advanced Encryption Standard (AES) or the likes [sic].” EX1005, 12:35–42.

Thus, the first embodiment involves data being aggregated at the data source before it is returned to the data aggregator, and the second situation involves de-identifying individual patient level data that can be returned to the data aggregator and later merged or linked by the aggregator itself. EX2001, 100–137. Notably, neither situation involves the data source entities performing token matching on de-identified patient data as alleged. *Id.* Dr. Clark’s characterization of these embodiments is completely at odds with Evenhaim’s actual disclosure. *Id.*; EX1003, ¶40.

The portion of Evenhaim that Dr. Clark cites states that “the person identity information ... is replaced with a unique encryption key,” but nothing in Evenhaim discloses or suggests that such replacement is to allow the unique encryption key (i.e., the alleged token) to be matched to another token in a query received from the aggregator. EX2001, 100–137. Even the sentence that Dr. Clark quotes in support of his position—“the person identify information, *for the matched population*, is replaced with a unique encryption key,” (EX1003, ¶40, citing EX1005, 12:39–41)—indicates that the individuals *are first matched* to determine the matched population before the person identity information, for the matched population, is replaced with a unique encryption key. EX2001, 100–137. As such, because the “token” is not even produced at the data source until after a

matching population is already identified, the portions relied on by Petitioner's witness cannot logically describe any token matching as alleged. *Id.*

Dr. Clark also distorts Evenhaim's descriptions of data linking *at the aggregator* to wrongly contend that the data source entities would create tokens associated with patient healthcare data for a matching process. *See* EX1003, ¶40 ("this token matching system 'preserves the ability to known [sic] that two records belong to the same identity, but preserves the privacy of the identity of that person.'"). *Id.*, 12:42–45. But Dr. Clark fails to acknowledge that Evenhaim is instead referring to the *aggregator's* (not the data sources') ability to link de-identified patient records belonging to the same patient:

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. Of course, special care must be taken that the entity performing the linkage is not capable of knowing the key and decryption function;

EX1005, 12:12–18.

Evenhaim's separate references to the "data sources" and the entity that is "further down the data processing circuit," makes clear that the latter entity is different from the data sources. EX2001, 100–137. And because Evenhaim seeks to prevent compromise of individual identities at the entity "further down the processing circuit," the phrase cannot encompass the data sources, which

themselves are covered entities under HIPAA that are already aware of such identities and already maintain PHI. *Id.*; EX1005, 5:12–28. As such, Dr. Clark’s statement that a “POSA would understand that ‘further down the data processing circuit’ describes the subsequent use of the de-identified records for querying,” is simply incorrect. At the very least, the cited portions of Evenhaim do not show that any token matching would take place at the data sources. EX2001, 100–137; *see also* EX2002, 55:3–16, 56:6–13 (Dr. Clark conflating background discussion with Evenhaim’s proposed solution).

For each of the reasons described above (*supra*, §IV.B.1–3), Evenhaim fails to disclose or render obvious multiple limitations of independent claims 1 and 7. EX2001, 100–137. For example, Petitioner equates the data aggregator of Evenhaim to “an encryption server.” Pet., 13. However, because Evenhaim does not describe that the data aggregator produces individual tokens either from the patient list and query or as part of the data-merger embodiments, Petitioner has not, and cannot, show that Evenhaim provides “an encryption server... for producing a token for each individual included in a group composed of multiple individuals,” as recited in elements [7.a]–[7.b] (and similarly in [1.b]–[1.c] and [14.c]–[14.d]). Pet., 17–18, 30; EX2001, 100–137.

Further, Petitioner equates Evenhaim’s data source entities to the “data server.” Pet., 19. However, because Evenhaim fails to describe any matching of

request tokens from the data aggregator to tokens for de-identified healthcare data at the data source entities, Petitioner has not, and cannot, show that Evenhaim provides “a data server for producing the requested healthcare information... by identifying the tokens in the set of de-identified healthcare data ... that correspond to the produced tokens,” as recited in elements [7.e]-[7.g] (and similarly in [1.f]-[1.g] and [14.f]-[14.g]). Pet., 19–20, 30; EX2001, 100–137.

Neither would the foregoing features be obvious over Evenhaim. EX2001, 100–137. To the extent Petitioner argues that it would have been obvious to modify Evenhaim to have the data source entities search de-identified healthcare information based on matching tokens associated with the de-identified healthcare information to request tokens from the data aggregator, the contention is unsubstantiated and improper. As described above, Evenhaim explicitly teaches against such an approach that would require the data sources to search on anything but the original micro-level patient data. *Supra*, §IV.B.1–2. Moreover, common knowledge of a POSITA may only be used to supply a missing claim limitation when that limitation is “unusually simple and the technology particularly straightforward.” *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361 (Fed. Cir. 2016). The Petition both fails to present any evidence that the above-noted limitations that are missing from Evenhaim were commonly known in the art and fails to show that these limitations are directed to unusually simple features. They

are not. Evenhaim’s system would require a substantial re-design to implement the embodiments that Petitioner and Dr. Clark attempt to import in the reference, which would require sophistication and complexity to achieve a technical design that both achieved Evenhaim’s specific goals and complied with applicable privacy laws and regulations. EX2001, 100–137. This is anything but simple. *Id.*

For each of these reasons, Petitioner has failed to establish that any independent claims 1, 7, or 14 are obvious over Evenhaim. Each of the dependent claims inherit the novelty and non-obviousness of the corresponding independent claim, and thus have not been shown to be obvious either. Ground 1 of Petitioner’s challenge should be dismissed. *Id.*

V. GROUND 2: THE EVENHAIM-SETTIMI COMBINATION FAILS TO RENDER THE CHALLENGED CLAIMS OBVIOUS

A. Overview of Settimi (EX1006)

Settimi describes systems and methods for searching electronic medical data to identify potential participants for clinical studies. EX1006, Abstract. The method allows for sending de-identified patient information between primary care provider (“PCP”) sites and a data warehouse. EX1006, [0009]; EX2001, 80–82.

Settimi’s system can also generate cohort reports across de-identified patient data stored in a data warehouse. EX1006, [0010]. In one embodiment, the cohort report can be sent back to a PCP and re-identified at the PCP site. EX1006, [0027]. Settimi’s de-identification process involves encrypting a patient identifier

with a unique password *at the PCP site*. EX1006, [0041]. Re-identification

likewise involves decrypting the encrypted patient identifier at the PCP site. *Id.*;

EX2001, 80–82.

B. Analysis

In Ground 2, the Petitions contends that the teachings of Evenhaim in view of Settimi would have rendered the claims of the '641 Patent obvious. Pet., 34–51. In the proposed Evenhaim-Settimi combination, the Petition states that Settimi’s central patient data warehouse would replace the individual data source entities in Evenhaim and the central patient data warehouse would search de-identified patient records by matching tokens representative of patients whose data was requested to stored tokens associated with the patients’ de-identified records. Pet., 35; EX1003, ¶52. According to the Petition, “Settimi describes *querying* the de-identified patient records *by using the token (EPID)* to find the associated records for a specific patient without revealing the patient’s identity.” *Id.* Not so. Settimi not only fails to describe querying using EPIDs as alleged, but the use of EPIDs for querying would be purely non-sensical in Settimi’s system, let alone in the Evenhaim-Settimi combination. EX2001, 138–144.

1. The Evenhaim-Settimi combination fails to disclose or render obvious multiple limitations of independent claims 1, 7, and 14

In more detail, Settimi describes techniques for querying de-identified medical data stored in the central warehouse to surface patients who fit the clinical trial criteria specified in the request. EX2001, 138–144. For example, to identify candidate patients for a clinical trial, a user can query for “patients with a particular disease that were treated with a particular medication,” “patients of a particular age and sex who have particular test results,” or “all women with heart disease who are taking a hormone replacement therapy drug.” EX1006, [0036]. A cohort of patients who meet the conditions specified in the request are identified from de-identified medical records stored in the central warehouse, and an indication of the cohort is returned to the requester or the primary care provider (PCP)—although only the PCP has the ability to re-identify patients by decrypting the EPIDs. *Id.*, [0037]. EX2001, 138–144.

Importantly, Settimi’s queries necessarily include and rely on patient characteristics to identify the cohort because Settimi attempts to eliminate the traditional “use of mass media to broadcast a need *for patients who fit a list of clinical conditions.*” EX1006, [0011]; EX2001, 138–144. Querying the database of Settimi using EPIDs—as Petitioner contends—would make no sense at least because EPIDs do not represent patient characteristics or clinical conditions that

would allow for identification of a cohort for clinical trials or other research as intended. EX1006, [0038]. Rather, as Petitioner and Dr. Clark admit, the database in Settimi is searched using a “common vocabulary” that normalizes terminology in the data from multiple sources. Pet., 36; EX1003, ¶137. Petitioner does not contend (and it would be meaningless to do so) that this common vocabulary includes EPIDs. It does not. Indeed, if particular EPIDs that fit the clinical study requirements were known to the entity generating the query, there would be no reason for the query in the first place. EX2001, 138–144.

Accordingly, much like Evenhaim, Settimi never discloses querying a database for de-identified healthcare data using tokens or performing so-called “token matching” at a de-identified data server, and Petitioner’s premise for combining the two references— namely, that “a POSA would readily understand that the search would involve matching the tokens sent in the query to the tokens already in the relevant healthcare record” is not correct. Pet., 41; EX1003, ¶153; EX2001, 138–144.

For at least these reasons, Settimi cannot cure the deficiencies of Evenhaim, and the Evenhaim-Settimi combination fails to render obvious at least the functions of a “data server” as recited in elements [7.e]–[7.g] (and similarly in [1.f]–[1.g] and [14.f]–[14.g]). Pet., 40–41, 46. Settimi and the combination likewise do not disclose or render obvious the claimed “encryption server” as

recited in elements [7.a]–[7.b] (and similarly in [1.b]–[1.c] and [14.c]–[14.d]), and neither the Petition nor Dr. Clark rely on Settimi for the encryption server features that are already lacking from Evenhaim. Pet., 37, 41; EX1003, 136–138; EX2002, 96:23–97:8; EX2001, 138–144.

2. The Evenhaim-Settimi combination would not have been obvious because integration of Settimi’s teachings would have violated Evenhaim’s express preference for searching original, micro-level patient data

The Petition’s proposed combination of Evenhaim and Settimi also would not have been obvious to a POSITA for the additional reason that it would have violated Evenhaim’s express preference and principle of operation for searching on original, micro-level data before de-identification and aggregation. EX1005, 6:15–34 (“instant invention allow[s] analysis of ‘source-entity’ raw data at its original, most detailed form (high resolution data) including full access to all of the privacy sensitive data currently at its disposal”), 17:42–52 (“analysis is performed on the original, most complete data set”), 17:28–41 (contrasting Evenhaim’s purported invention with “classic” approaches that called for “aggregation of de-identified patient” before searching); EX2001, 138–144; EX2002, 51:8–17 (“that’s sort of the point of the reference, right?”).

For example, regarding the combination, the Petition contends that “[o]nce de-identified and stored in the central repository, the healthcare records can be queried using a token matching scheme ... using the token (EPID) to find the

associated records for a specific patient without revealing the patient’s identity.”

Pet., 35. As described in the preceding section, Settimi never actually discloses searching the data warehouse using the token (EPID). EX2001, 138–144. But even if Settimi did disclose these features, the combination still would have required a non-obvious modification to Evenhaim’s system in light of Evenhaim’s desire to search “raw data at its original, most detailed form.” EX2001, 138–144. The data records stored in Settimi’s central warehouse are not maintained in their original, most detailed form and do not include PHI. Not only is the data de-identified, thereby leaving the data records without useful information that Evenhaim sought to make available for search, but Settimi confirms that the data imported to the data warehouse before a search would be performed is aggregated, cleansed, and normalized—all contrary to Evenhaim’s express teachings. EX1006, [0035] (“The data import function 206 *aggregates* and *cleanses* de-identified patient data from multiple sites and then stores the data into a staging area 208. Data received from multiple PCP systems 108 is *normalized*’ and “*combined together* into a relational database”); EX2002, 96:2–20. Ground 2 thus fails for this additional reason. EX2001, 138–144; *Galderma*, 737 F.3d at 738; *Polaris*, 882 F.3d at 1069; *Plas-Pak*, 600 Fed. Appx. at 758–759; *In re Ratti*, 270 F.2d at 813; IPR2016-01842, Paper 35 at, 39, 53.

VI. GROUND 3: THE DICK-LANDI COMBINATION FAILS TO RENDER THE CHALLENGED CLAIMS OBVIOUS

A. Overview of Dick (EX1007)

Dick describes computer-based technologies for retrieving medical records over a network. EX1007, [0002], [0010], [0021]–[0022]; EX2001, 83–89. The topology of Dick’s system is illustrated in FIG. 3:

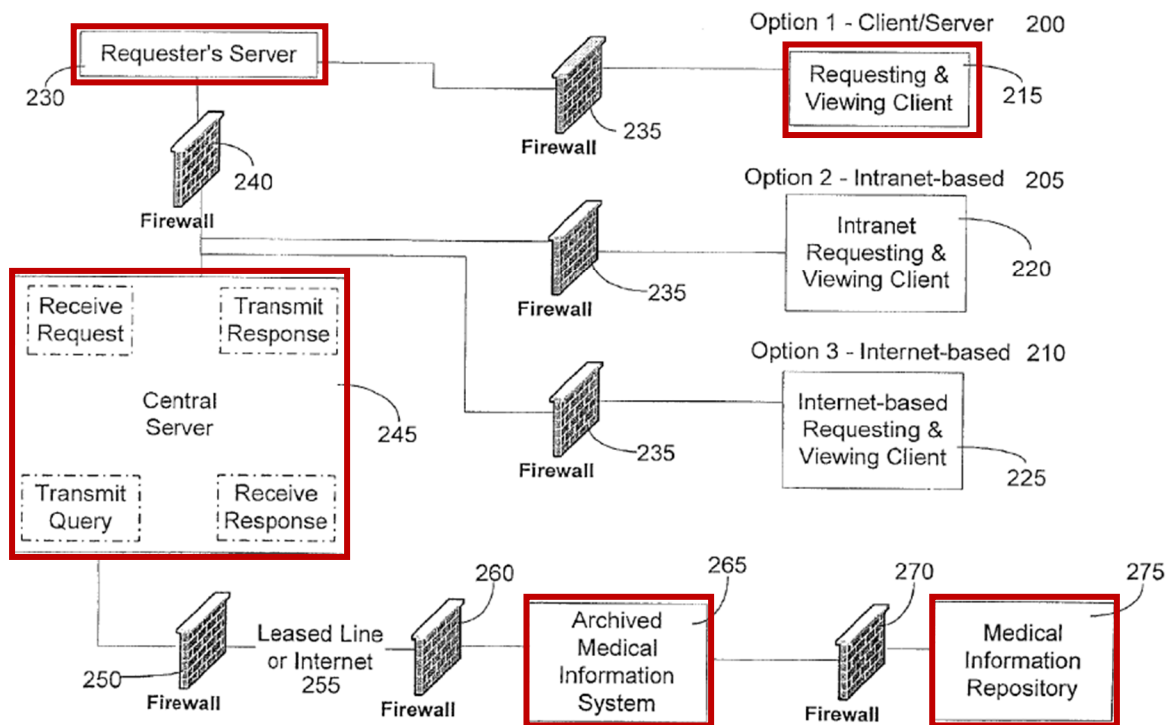


FIG. 3

EX1007, FIG. 3 (annotated)

The Petition focuses on Option 1 – Client/Server. Pet. 55. In this embodiment, the requesting and viewing client (RVC) 215 is “a terminal having at least a video display and keyboard. In general, each RVC is operated by an

authorized user to request and subsequently review retrieved medical information or other search results.” EX1007, [0021]. The RVC 215 can “receive a request from an authorized user responding to prompts from software executing on requester’s server 230.” EX1007, [0022]. Notably, this is the **only** function attributed to the requester’s server 230 in the entirety of Dick’s disclosure. EX2001, 83–89; EX2002, 75:19–24.

In Dick, “[e]ach request for medical information includes identification of a subject,” where a “subject might consist of a human individual or group of humans.” EX1007, [0024]. Thus, in Dick, the requests do not include tokens or encrypted IDs, but rather, they include individual identification information or identification information for a group. EX2001, 83–89.

After receiving the request, the requester’s server forwards the request to a central server 245. EX1007, [0027]. Then, the central server 245 sends a query based on the request to a medical information repository (MIR) 275 that stores protected health information (“PHI”) for patients. EX1007, [0028]–[0029]. The MIR 275, which would be a covered entity under HIPAA, locates data records responsive to the query and returns them in a response to the central server 245; the central server then sends the records to the requesting client through the requester’s server. EX2001, 83–89; EX2002, 74:6–11, 75:19–78:19; 93:5–94:7.

In other embodiments, the central server 245 sends the query to an archive

medical information system (AMIS) server 265 to reduce the computational burden on the MIR. EX1007, [0028]. The AMIS server searches using the “identification of an individual for whom a request is being made” and thus the query must include “identification” of the subject. EX1007, [0029].

When MIR 275 does not have authorization from the subject for release of their healthcare information, Dick discloses that the records are de-identified before being released to the central server 245. EX1007, [0045]–[0046], FIG. 2.

Dick does not describe tokenization here, nor elsewhere. To the contrary, Dick’s searching of medical data records explicitly depends on knowledge of the names or other individually information of any individuals identified in the request. EX1007, [0029] (discussing UMPI and L-MPI). For example, Dick teaches that the central server can even maintain a Universal Master Person Index (UMPI) that includes a set of demographics and other specific information for identifying individuals. EX1007, [0029].

Dick does discuss de-identification. EX2001, 89, 146–152; EX2002, 79:17–81:2. Absent consent for release of medical records, medical records must be de-identified. EX1007, [0045]–[0046]. Dick explains that de-identification can occur “at one of any number of points, including being de-identified at the originating source of the information,” *but* “in any case, the information must be de-identified prior to being released or distributed.” EX1007, [0046]. For

example, the MIR or AMIS must de-identify the requested information before returning the information to the central server. *Id.*; EX2002, 77:5–78:19.

Importantly, in Dick, the searching is performed using names, but the results are de-identified if the query does not include some indication of patient consent.

EX1007, FIGS. 1–2; EX2001, 83–89.

B. Overview of Landi (EX1008)

Landi describes “secured key encryption for de-identifying patient data to ensure patient privacy, while allowing only the owners of the patient data records and/or other legally empowered entities to re-identify subject patients of de-identified data records, when needed.” EX1008, 1:13–22; EX2001, 90–95.

Landi recognized that various approaches to de-identifying information under the HIPAA Privacy Rule were known by the time of its priority filing in March 2003. EX1008, 2:19–26. Landi perceived a problem with these approaches in that they lacked any “mechanism by which patient identification can be recovered, if necessary.” EX1008, 2:19–26. Landi thus proposed techniques for de-identifying PHI that would further allow the PHI to be re-identified by authorized entities as needed. *Id.*, 2:36–40; EX2001, 90–95. This framework for re-identifying patients from de-identified health information was indeed a core concern of Landi’s. EX1008, 2:36–40, 2:49–53, 3:9–13, 3:42–57, 4:28–34, 4:35–48, 4:54–64, 6:56–7:2, 7:30–38, 7:43–48, 8:5–10, 8:16–37, 8:38–

55, 9:10–16, 9:36–42, 10:12–14, 10:32–37; EX2001, 90–95.

FIG. 1 illustrates an embodiment of Landi's system:

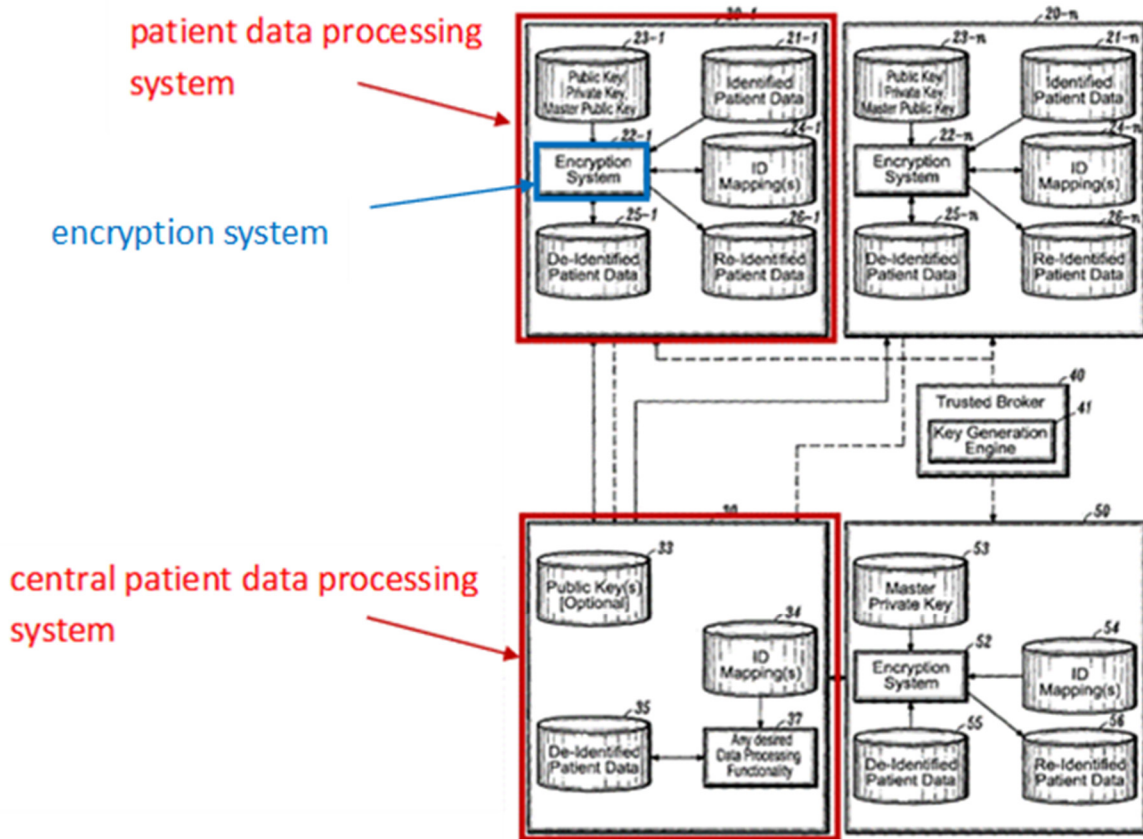


FIG. 1

EX1008, FIG. 1 (annotated)

Landi explains that “[t]he patient data processing systems (20-1–20-n) are operated at different clinical sites by different healthcare organizations (including, but not limited to, doctors, healthcare providers, institutions, associations, organizations, hospitals, etc.).” EX1008, 4:19–23. The patient data processing systems 20-1–20-n maintain identified patient data (21-1–21-n), which constitute protected health information (“PHI”) under HIPAA, and the patient data

processing systems would therefore qualify as “covered entities.” EX2001, 90–95; EX2002, 87:24–88:2.

Each patient data processing system further includes a respective encryption system (22-1–22-n) that implements a “secure public encryption protocol (e.g., RSA).” EX1008, 4:49–67. The encryption systems reside at the patient data processing systems and “encrypt[] patient identifying information that is stored in (or stored with) the patient data records (21-1-21-n) using respective public keys and/or a master public key (23-1-23-n)” to produce Encrypted IDs. EX1008, 5:3–7; EX2002, 86:25–87:9. Encrypted IDs are stored “with or within a corresponding de-identified [] patient data record (i.e., a patient data records from which patient identifying information has been removed).” EX1008, 5:32–44. Nowhere does Landi teach or suggest maintaining Encrypted IDs apart from the corresponding de-identified patient data record. EX2001, 90–95. Nor does Landi ever describe that the Encrypted IDs would be used for “token matching,” despite the Petition’s unsubstantiated assertions to the contrary. *Id.* This is because Landi is not about performing searches or token matching; instead, Landi is about de-identifying health records using a technique that facilitates re-identification. EX1008, 2:36–40, 2:49–53, 3:9–13, 3:42–57, 4:28–34, 4:35–48, 4:54–64, 6:56–7:2, 7:30–38, 7:43–48, 8:5–10, 8:16–37, 8:38–55, 9:10–16, 9:36–42, 10:12–14, 10:32–37.

The encryption system further includes capabilities to “re-identify[] subject patients by using [an] appropriate private key to decrypt de-identified patient data that is contained in de-identified patient data records (25-1–25-n).” EX1008, 6:56–7:2. Landi describes that “holders of valid private keys (e.g., owners of the patient data, or legally empowered entities) [can] decode the de-identified patient data and re-identify patients.” EX1008, 8:44–46.

Landi also provides a central patient data processing system 30 that stores de-identified patient data released from the patient data processing systems, “wherein the collected de-identified data records can be processed for purposes of e.g., research, health care monitoring, etc.” EX1008, 4:26–28. Landi emphasizes that “the entity (or entities) that operate the central patient data processing system (30) *does not have the authority to re-identify subject patients* that are associated with the de-identified patient data records (35)” and accordingly, “the central patient data processing system (30) does not include an encryption system that is capable of decrypting Encrypted IDs that are stored in or with the de-identified patient data records (35).” EX1008, 7:22–38; EX2001, 90–95.

C. Analysis

The Petition fails to show that the Challenged Claims are unpatentable over

the Dick-Landi combination for multiple reasons, as described below.⁴ EX2001, 145–198.

1. The Petition fails to demonstrate a motivation to combine Dick and Landi

The Petition fails to establish that a POSITA would have combined Dick and Landi in the manner of the Challenged Claims of the '641 Patent. EX2001, 146–152, 170–198. Indeed, the Petition’s entire basis for combining Dick and Landi is not at all true, and no record basis exists to combine Dick and Landi in the manner proposed. *Id.* Petitioner cannot meet its burden of demonstrating obviousness based on the Dick-Landi combination when it cannot even show that a POSITA would have combined the references as alleged.

More specifically, the core of the Petition’s proposal to combine Dick and Landi is underpinned by the erroneous assertions that “Dick does not describe any specific de-identification methods,” and therefore, a “POSA relying on Dick would naturally look elsewhere in order to implement the de-identification called for in Dick.” Pet.52; EX1003, ¶¶201–203; EX2002, 79:17–81:2. This is simply not true. Dick clearly describes specific methods for de-identifying healthcare

⁴ The deficiencies described in this section are similarly applicable to the claims challenged in Ground 4 based on the Dick-Landi-Murphy combination.

records, and a POSITA would not have had any reason to look beyond Dick to find such methods. EX2001, 145–152; EX2002, 80:21–25.

For example, at paragraph [0045], Dick explains that de-identification can involve not only removing names or addresses of patients, but also removing “all ‘Identifying’ information” such as:

[I]dentifiers of the individual or of relatives, employers, or household of members of the individual associated with the record, which identifiers include names, geographic subdivisions, elements of dates related to any individual, telephone numbers, fax numbers, e-mail addresses, Social Security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate license numbers, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, photographic images, any other unique identifying number, characteristic or code.

EX1007, [0045]. Even Petitioner’s witness, Dr. Clark, conceded this fact:

11 Q. Would a person of skill know how to implement
12 the de-identifying methodologies?

13 A. Should.

21 Q. Would a person of skill see a need to look
22 beyond the Dick reference itself to implement
23 de-identifying methodologies?

24 A. No. I think a person of skill would have
25 knowledge of HIPAA and the need to de-identify data.

EX2002, 80:11–25; *see also id.*, 79:17–81:2.

Likewise, Landi recognizes that some “methods for de-identifying patient data include *simply stripping all information* from the patient data records that can be used to determine the identity of a patient,” like in Dick. EX1008, 2:19–26. In this way, Dick teaches de-identification techniques sufficient for a POSITA to perform de-identification on health information. EX1007, [0045]; EX1008, 2:19–26; EX2001, 146–152; EX2002, 79:17–81:2.

To be sure, Dick goes beyond “simply stripping” identification information, as Landi puts it. Dick also teaches a mechanism for de-identification technique for situations when removing information “is not practical or renders the data useless.” EX1007, [0045]; *see also id.*, [0046]–[0047]. The Petition’s assumption that “Dick does not describe any specific de-identification methods” is thus patently false. A POSITA would have found the de-identification methodology taught by Dick sufficient and would have had no reason to turn to Landi (or

elsewhere) to solve this problem as alleged. EX2001, 146–152; EX2002, 79:17–81:2. Indeed, the law is clear that there can be no motivation to combine where, as here, the stated problem does not actually exist or the stated problem is already addressed by the primary reference. *See, e.g., Amerigen Pharms. Ltd. v. UCB Pharma GmbH*, 913 F.3d 1076, 1081, 1087–87 (Fed. Cir. 2019) (affirming the Board’s finding of no motivation to combine when no problem existed); *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F. 3d 1342,, 1368–69 (Fed. Cir. 2012) (“Because each device independently operates effectively, a [POSITA], ... would have no reason to combine the features of both devices into a single, device.”); *Runway Safe LLC v. Engineered Arresting Sys’s*, IPR2015-01921, Paper 9 at 6–10 (PTAB Feb. 29, 2016) (holding no motivation to combine because a POSITA would have had no reason to solve a problem that does not exist: “[b]ecause we are not persuaded that water intrusion is a problem in Gwynne’s arrester system, we are not persuaded by Petitioner’s proffered rationale[.]”).

The Petition also contends that a POSITA would have turned to Landi because “[l]ike Dick, Landi’s purpose is compliance with HIPAA.” Pet., 53. But Landi’s approach is not, in fact, HIPAA compliant. Under 45 C.F.R. §164.514(c)(1), “[a] covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that: ... [t]he code or other means of

record identification *is not derived from or related to information about the individual* and is not otherwise capable of being translated so as to identify the individual.” Notwithstanding these plain requirements of HIPAA, the Petition relies on Landi’s de-identification method that involves “generating an encrypted ID for the individual, *wherein the encrypted ID comprises an encrypted representation of one or more items of individual identifying information.*”

EX1008, 2:46–48; *see also id.*, 5:13–19; EX2001, 170–173. By generating and releasing reversibly Encrypted IDs based on individual identifying information of patients, Landi blatantly violates HIPAA’s proscription against assigning codes for re-identification that are “derived from or related to information about the individual.”⁵ 45 C.F.R. §164.514(c)(1). A POSITA therefore would not even turn to Landi for its specific de-identification methodology that involves creating Encrypted IDs because Landi’s approach would not have achieved the Petition’s stated goal of achieving HIPAA compliance. Landi instead invites a HIPAA violation, which a POSITA would have sought to avoid. EX2001, 146–152, 170–

⁵ The Petition’s reliance on Settimi in Ground 2 suffers from a similar defect that spoils the proposed Evenhaim-Settimi combination. Like Landi, Settimi generates its encoded patient identifier (EPID) based on information about the individual. *See* EX1006, [0038], [0041]–[0043], [0056].

198.

For each of these reasons, a POSITA would have lacked motivation to combine Dick and Landi in the manner proposed in the Petition. *Id.*

2. The Dick-Landi combination does not disclose or render obvious elements [1.b]-[1.c], [7.a]-[7.b], or [14.c]-[14.d]: an encryption server for producing a token for individuals in a group identified in a request for healthcare information

The Petition next fails to establish that the Dick-Landi combination discloses or renders obvious “an encryption server, having a processor and a memory, 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,” as recited in elements [7.a]–[7.b], or similarly recited in [1.b]–[1.c] and [14.c]–[14.d]. EX2001, 153–162. To reach these claim elements, the Petition argues that it would have been obvious to implement an encryption server akin to Landi’s encryption system 22 in Dick’s requester’s server 230. Pet., 55–57. But this theory is misplaced for multiple reasons. EX2001, 153–162.

At the outset, considered individually, neither Dick nor Landi describes an encryption server that produces a token for each individual included in a group identified in a request for healthcare information, as claimed. EX2001, 153–162. It is undisputed that Dick lacks these features and the Petition does not rely on Dick in this regard. The Petition instead turns to Landi, but at best, Landi describes an encryption system *located only within a patient data processing*

system 20—i.e., a covered entity under HIPAA—and nowhere else. EX1008, 4:49–54, 5:7–13 (describing that the “healthcare entity” can use its own public key to generate an Encrypted ID), 5:32–41 (describing the data processing system generating Encryption IDs and storing them in a repository), 6:56–7:2 (describing that each healthcare entity that releases de-identified patient data records can securely store a respective private key for purposes of re-identifying patient data); FIG. 1; EX2002, 86:25–87:7 (describing encryption occurring at the patient data processing systems in Landi).

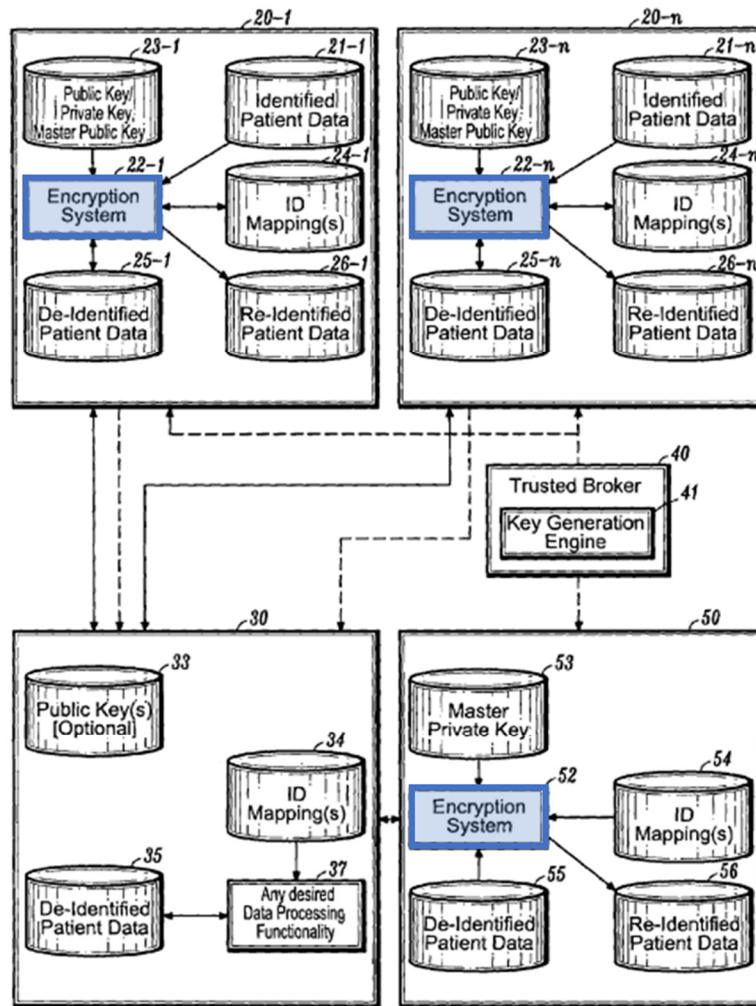


FIG. 1

EX-1008, FIG. 1 (annotated).

In this context, it would not have been obvious to implement the encryption system of Landi at the requester's server of Dick. The Petition's proposal to the contrary is instead borne of impermissible hindsight, as evidenced by the following facts. EX2001, 153–162.

First, the Petition's proposal for implementing encryption at Dick's

requester's server is predicated on an assumed need for the requester's server to provide tokens rather than patient names to the next server in the network for HIPAA compliance (e.g., Dick's central server 245 or Landi's central system 30). Pet., 57–58 (“it would potentially violate HIPAA to just send PII to be used for such a query directly to the centralized data server”). But that need is entirely illusory, conspicuously devoid of evidentiary support. EX2001, 153–162. To the contrary, as Dr. Clark conceded at his deposition, there would be no HIPAA violation in sending only PII in a query to the requester's server:

16	Q. Sure. So I'll rephrase my question.
17	Are you -- are you aware of any provisions of
18	HIPAA that would be violated by a noncovered entity
19	transmitting patient names to covered entities?
20	A. I mean, I'd have to look at the specific
21	example. But if you just sent the name and didn't have
22	the healthcare data with it in any way, then it wouldn't
23	violate. But if you link that with any medical
24	procedure or any healthcare information, then you would
25	have a HIPAA violation.

EX2002, 57:16–25

There is in fact NO rule in HIPAA that prevents the transmission of PII in a query from a non-covered entity like Dick's requester's server, especially when the query includes no PHI. EX2001, 153–162, EX2006, §164.514(d); EX2002, 57:16–25, 60:12–23. Accordingly, the potential for a HIPAA violation by issuing queries from the requester's server in Dick simply does not exist as a problem at

all. This point was reinforced by Dr. Clark’s further admission that encryption could alternately be performed at Dick’s central server rather than the requester’s server without incurring a HIPAA violation. *See* EX2002, 92:3–21. Lacking the problem of a potential HIPAA violation in the first place, the Petition cannot support the claim that a POSITA “would have been motivated to use Landi’s encryption server to produce tokens to query against a de-identified patient database requester.” Pet. 53 (citing EX1003, ¶203); *see, e.g., Amerigen Pharms. Ltd.*, 913 F.3d at, 1081, 1087–87.

Second, the Petition’s reliance on impermissible hindsight in placing an encryption system in Dick’s requester’s server is highlighted by the substantially different functions and contexts in which Landi’s encryption system exists as compared to how the Petition proposes to implement encryption in the Dick-Landi combination. EX2001, 153–162. Landi describes the encryption system 22-1–22-n as being for de-identifying (and re-identifying) patient records at the patient data processing systems 20-1–20-n, and stores the Encrypted IDs with or in patent data records. EX1008, 5:3–7, 5:32–47, 6:56–65, 7:26–30, 8:38–55, 13:4–12. The patient data processing systems 20-1–20-n are covered entities under HIPAA, per Dr. Clark. EX2002, 87:24–88:2. Landi makes it clear that the encryption system performs de-identification at a covered entity that also stores PHI. Nowhere in Landi does it describe the encryption systems as being configured to generate

tokens from a received query and to send the query onwards. EX2001, 153–162.

Nor does it describe placing the encryption system anywhere besides a covered entity for the purposes of de-identifying patient data, as the Petition proposes to do with encryption at Dick’s requester’s server. EX2001, 153–162. If anything in Dick’s system is analogous to the patient data processing systems 20 where encryption occurs in Landi, it would be Dick’s medical information repository 275 or AMIS 265 since they too are covered entities that maintain patient’s PHI.

EX1007, [0028], [0045]-[0046]; EX2002, 85:5–86:4. But the Petition inexplicably proposes to place the encryption server at Dick’s requester’s server, which is not at all analogous to Landi’s patient data processing systems 20.

EX2001, 153–162.

Third, the Petition fails to recognize that the proposed combination itself invites a HIPAA violation since the system would impermissibly release to the requester’s server information sufficient for it impermissibly correlate de-identified patient records with the patients to whom they belong: the names of the patients received from the request, the corresponding encrypted IDs, and the patients’ de-identified healthcare information received in the response. EX2001, 153–162; EX2002, 76:6–78:19, 92:16–21, 93:16–22. The MIR/AMIS being covered entities would not be permitted to send de-identified medical information to the requester’s server because the requester’s server is not authorized to have

such information. EX2001, 153–162; EX2002, 74:9–17. Dick never proposed that the requester’s server would maintain patients’ PHI, and the Petition has certainly not established that the requester’s server would be authorized to do so. EX2001, 153–162; EX2002, 71:20–72:6. Accordingly, it would be impermissible for the MIR/AMIS to release all of this information to the requester’s server that could be used to link patient names with their corresponding healthcare records. EX2001, 153–162. The risk of HIPAA violations arising from the proposed combination indicates that a POSITA would not consider this option at all. EX2001, 153–162.

For each of these reasons, the Dick-Landi combination fails to disclose or render obvious the claimed features of the “encryption server” as recited in elements [7.a]–[7.b], or the features similarly recited in [1.b]–[1.c] and [14.c]–[14.d]. EX2001, 153–162.

3. The Dick-Landi combination does not disclose or render obvious elements [1.f], [7.e]–[7.f], [14.f]: identifying tokens in a set of de-identified healthcare data that correspond to request tokens for individuals in a group

The Dick-Landi combination next fails to render the Challenged Claims obvious because it fails to provide the steps of “producing the requested healthcare information that characterizes the group 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” (elements [1.f], [14.f]) or “a data server

for producing the requested healthcare information that characterizes the group 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” (element [7.f]). EX2001, 163–168.

As an initial matter, the claims are not directed to mere “token matching” or “de-identification” as alleged in the Petition. *See* Pet., 6, 52, 59, 63. The claims instead involve a novel combination of techniques in a particular context in which, among other things, requested healthcare information is produced by identifying the tokens in a set of de-identified healthcare data that correspond to tokens produced for individuals identified in a request for healthcare information that characterizes a group. The Petition has not demonstrated that either Dick or Landi discloses or suggests these claim features, whether alone or in combination. EX2001, 163–168.

For example, the Petition cites to Landi’s teachings at 8:23–55 and 11:23–29 for these features. Pet., 62–63. But these portions of Landi do not involve matching tokens in the manner claimed, or even matching Encrypted IDs. This portion of Landi instead describes how use of the same encryption algorithm and public key to encrypt the same PII from two or more data records belonging to the same patient will produce the same Encrypted ID, thereby ensuring consistency *in the assignment* of Encrypted IDs to the same patients’ records from different

providers or at different times. EX1008, 8:23–55 (Since the encryption is reproducible, the same patient can be recognized at different times (i.e., *consistent de-identification can be achieved* over episodic collection events) even though the identity of the person remains unknown.”), 11:3–29 (describing step 53 where Encrypted IDs are generated by the encryption system at the patient data processing system, and clarifying that the “process ensures that if data is collected more than once *from a particular patient*, the patient will be mapped to the same Encrypted ID”); EX2001, 163–168. This mapping and generation of Encrypted IDs, and collection of patent records, notably occurs at the patient data processing system 20-n, and not at the central patient data processing system 30. *Id.*, 8:23–55, 11:3–29, cls.1,3,12,15.

The Petition’s additional citation to Landi’s Claim 15 is deficient for similar reasons. Pet., 58–60. The operations described in claim 15 would be performed at the patient data processing systems 20-1–20-n where de-identification and re-identification occur, and do not involve matching encrypted IDs produced in a query to encrypted IDs associated with de-identified health care data stored in the central patient data processing system 30. *See*, EX1008, 8:49–55, cl. 1,3,12,15.

To be clear, the Petition has not even shown that Landi expressly teaches querying the central data processing system 30 at all. EX2001, 163–168. At best, Landi teaches that “structured” patient data records can be “readily searched” for

the purposes of de-identification at the patent data processing system 20-1–20-n.

EX1008, 11:52–63. Likewise, unstructured patient data records can be searched for the same purpose. EX1008, 13:13–40. But Landi does not disclose that the central patient data processing system 30 would ever be searched in the manner claimed, and it is wrong to assume that Landi teaches token matching at the central data processing system 30 at all—especially when Landi does not even disclose querying the central patient data processing system 30 based on the Encrypted IDs in the first instance. EX2001, 163–168.

In short, the Petition has not shown that the Dick-Landi combination discloses or renders obvious the claimed operations for identifying tokens in a set of de-identified healthcare data that correspond to the produced tokens according to the features recited in elements [1.f], [7.e]–[7.f], and [14.f]. *Id.*

4. The Dick-Landi combination does not disclose or render obvious elements [1.h], [7.h], [14.h]: the produced healthcare information is absent personally identifiable information

During his deposition, Dr. Clark testified that in Landi, as applied to the combination, personally identifiable information (PII) is not “absent” from the produced healthcare information. Instead, the PII remains in the produced healthcare information as encrypted information (e.g., an encrypted ID). EX2002, 93:23–94:7.

23 Q. And so that de-identified information in Landi
24 is -- includes the encrypted ID, correct?
25 A. It could.
1 Q. In the combination, the encrypted ID would be
2 routed to the requesting client through the requester's
3 server?
4 A. That's possible, sure.
5 Q. That's consistent with your description of the
6 combination?
7 A. I think so.

And as mentioned before, Landi's encryption methodology is designed to permit re-identification of PII. *See, supra* §VI.B. Thus, consistent with Dr. Clark's explanation, PII is available in the produced healthcare information of the Dick-Landi combination and could be read simply by applying the decryption algorithm and re-identification techniques expressly described in Landi. EX1008, 2:36–40, 2:49–53, 3:9–13, 3:42–57, 4:28–34, 4:35–48, 4:54–64, 6:56–7:2, 7:30–38, 7:43–48, 8:5–10, 8:16–37, 8:38–55, 9:10–16, 9:36–42, 10:12–14, 10:32–37. The Dick-Landi combination therefore does not teach that the PII is ***absent*** from the produced healthcare information as claimed in elements [1.h], [7.h], or [14.h]. EX2001, 169.

VII. GROUND 4: THE DICK-LANDI-MURPHY COMBINATION FAILS TO RENDER THE CHALLENGED CLAIMS OBVIOUS

A. Overview of Murphy (EX1009)

Murphy describes “a model for obfuscation of data when served to a client application,” that purportedly “make[s] it extremely unlikely that an individual will be identified.” EX1009, 552; EX2001, 96–98. According to Murphy, the model can be implemented in a query tool that queries “a clinical data warehouse named the Research Patient Data Registry.” EX1009, 552.

To “prevent[] the identification of individuals in the database,” Murphy considered the option of “de-identify[ing] patients in the data base with a system that complies with HIPAA’s 18 points for data de-identification,” but Murphy finds this approach problematic. EX1009, 553. Rather than pursue de-identification, Murphy’s query tool instead limits the data returned in response to a query to an indication of “the **number** of distinct patients” identified in the database as satisfying the request. *Id.*

Moreover, to prevent users from being able to use the query tool to identify individuals, Murphy proposed “having the server ***not pass true numbers of patients to the query tool***, but rather numbers that would be ... distributed around the true number of patients [if the same query were performed repeatedly].” EX1009, 553–54. Murphy refers to this approach as “obfuscation,” which involves “creat[ing] small values that will be added or subtracted from the true

number of patients to prevent patient identification.” EX1009, FIG. 2. “In order to find the true number, one would need to run the same query repeatedly”—and Murphy’s tool would recognize such a repeated query as an attack. EX1009, 554. Put simply, Murphy does not return patient records; instead, Murphy returns an obfuscated **number** of patients identified in response to a query. EX2001, 96–98.

The Petition relies on an aspect of Murphy’s disclosure in which the results of a query are close to zero. Pet., 68–69. In that case, Murphy teaches modifying the “range algorithm to have a wider obfuscation at values close to zero, and [indicating] the greater range by returning ‘<3’ when the obfuscated number is less [than] 3.” EX1009, 555. Note that nowhere in Murphy does it block a query based on a number of patients in the query. EX2001, 96–98. To the contrary, even if the results to the query are a small (close to zero) number of patients, the Murphy obfuscation algorithm still returns a response that bears a relationship to the true number of patients identified in response to the query. EX1009, 555; EX2001, 96–98.

B. Analysis

The Petition relies on Murphy for elements [1.e], [5], [11], [12], [14.e], and [18]. Pet., 68–74. In analyzing claim 11, the Petition merely provides the

following terse explanation⁶:

Murphy makes clear that, in complying with HIPAA, an algorithm preferably blocks queries that return fewer than 3 patients to prevent the user from associating the patient with a particular record. Ex. 1009, 555. (“[W]e modify our range algorithm to have a wider obfuscation at values close to zero, and indicate the greater range by returning ‘<3’ when the obfuscated number is less than 3.”); Ex. 1003, ¶242. Ensuring a minimum number of tokens are identified would have been a simple design choice to comply with HIPAA. Ex. 1003, ¶¶66, 239-40.

Pet., 69.

The Petition’s analysis is problematic for multiple reasons and fails to show that the Dick-Landi-Murphy combination would have rendered obvious the features of the above-listed claim elements. EX2001, 199–204.

First, the Petition’s assertion that Murphy’s algorithm “blocks queries” when the number of patients is less than 3 is incorrect. EX2001, 199–204; EX2002, 68:10-69:2. For results around zero, Murphy teaches modifying the “range algorithm to have a wider obfuscation at values close to zero, and

⁶ The Petition simply cites back to this same discussion from claim 11 without more when mapping the additional features recited in each of [1.e], [5], [12], [14.e], and [18]. Pet., 68–71. Notably, the Petition fails to address any of the differences in claim scope between these elements or explain how Murphy meets the specific limitations recited in each element.

[indicating] the greater range by returning ‘<3’ when the obfuscated number is less [than] 3.” EX1009, 555. Widening the obfuscation range in these cases is far different from blocking a query as alleged. To the contrary, the query tool always returns a numerical result to the query by applying an obfuscation algorithm. The obfuscation algorithm for results less than three involves providing an indication that the obfuscated result is less than three, rather than returning an absolute value or no value at all. The query is still answered, however, as the result informs the requester that the number of matching patients is near zero, and even this result bears a relationship to the true number of patients identified in response to the request. EX2001, 199–204. Importantly, Murphy’s query tool does not return actual patient records, but instead returns numerical values. *Id.* So, any numerical result, including ‘<3,’ constitutes a response to the query. *Id.* Accordingly, Murphy does not teach “blocking queries,” as argued by the Petition.

Second, the fact that Murphy’s query tool returns an “obfuscated” number of patients and makes its decision whether to apply wider obfuscation based on whether the “**obfuscated number** is less than 3” means that Murphy does not operate based on “a minimum number of individuals” or a “minimum number of corresponding tokens” as claimed. *Id.* The claims relate to a minimum number of individuals in the group or in the corresponding tokens—not “obfuscated” numbers as described in Murphy. Even if Murphy did “block queries” when there

are fewer than a certain number of patients in the obfuscated result (which it does not), the decision whether to block such queries would be based on some obfuscated number of patients rather than the number of individuals in the group or a minimum number of corresponding tokens as claimed. Thus, Murphy is simply inapplicable to the claimed features.

Finally, the Petition has not established that it would be obvious to combine Murphy’s teachings with the system of Dick and Landi. *Id.* Dick and Landi each describe systems that involve de-identifying patient data and making that de-identified data accessible to researchers and other interested users. *Supra*, §VI.A-B. Murphy does no such thing. Murphy explicitly considered and rejected the option of “de-identify[ing] patients in the database.” Murphy also rejects techniques where the patient information is susceptible to re-identification, like in Landi. EX1009, 553. Instead, Murphy opted to provide a query tool that would merely respond with a simple, obfuscated number of patients that match the search criteria without ever returning de-identified health records. Murphy’s obfuscation of the number of patients returned by a query tool in this context is completely different from Dick and Landi, and it would not have been obvious to condition the processes or results of Dick and Landi based on Murphy’s teachings in this regard. *ActiveVideo Networks, Inc.*, 694 F.3d at 1327; *InTouch Technologies, Inc.* 751 F.3d at 1352.

Therefore, and for each of these reasons, challenged claims are patentable over the Dick-Landi-Murphy combination. EX2001, 199–204.

VIII. CONCLUSION

For each reason stated herein, the Petitioner has not shown by a preponderance of the evidence that any claim of the '641 patent is unpatentable.

Respectfully submitted,

Dated 10/07/2024

/Nicholas W. Stephens/

W. Karl Renner, Reg. No. 41,265

Jeffrey J. Barclay, Reg. No. 48,950

Nicholas Stephens, Reg. No. 74,320

Fish & Richardson P.C.

60 South Sixth Street, Suite 3200

Minneapolis, MN 55402

T: 202-783-5070

F: 877-769-7945

Attorneys for Patent Owner

CERTIFICATION UNDER 37 CFR §42.24(d)

Under the provisions of 37 CFR §42.24(d), the undersigned hereby certifies that the word count for the foregoing Patent Owner's Response to Petition totals 13,991, which is less than the 14,000 allowed under 37 CFR §42.24(b)(1).\

Respectfully submitted,

Dated 10/07/2024

/Nicholas W. Stephens/

W. Karl Renner, Reg. No. 41,265

Jeffrey J. Barclay, Reg. No. 48,950

Nicholas Stephens, Reg. No. 74,320

Fish & Richardson P.C.

60 South Sixth Street, Suite 3200

Minneapolis, MN 55402

T: 202-783-5070

F: 877-769-7945

Attorneys for Patent Owner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§42.6(e), the undersigned certifies that on October 7, 2024, a complete and entire copy of this Patent Owner's Response and accompanying exhibits were provided by email to Petitioner by serving the correspondence email address of record as follows:

Justin Oliver
Nicholas Marcello
Michael Sandonato
VENABLE LLP
151 W. 42nd Street, 49th Floor
New York, NY 10036

E-mail: Datavant-IPRs@Venable.com

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667