

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DATAVANT, INC.

Petitioner

v.

VIGILYTICS LLC

Patent Owner

IPR2024-00226

Patent No. 9,118,641

Title: De-Identifying Medical History Information for Medical Underwriting

**PETITION FOR *INTER PARTES* REVIEW UNDER 35 U.S.C. §§ 311–319
AND 37 C.F.R. §§ 42.100 *et seq.***

TABLE OF CONTENTS

1.	Mandatory Notices.....	1
a.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)	1
b.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	1
c.	Lead and Backup Counsel and Service Information Under 37 C.F.R. §§ 42.8(b)(3)-(4)	1
d.	Payment of Fees Under 37 C.F.R. §§ 42.15(a) & 42.103.....	2
2.	Introduction.....	2
3.	Grounds for Standing.....	4
4.	Discretionary Denial is Not Appropriate.....	5
5.	Overview.....	5
a.	State of the Art	5
6.	The '641 Patent.....	7
a.	Construction of the Challenged Claims	7
b.	Person of Ordinary Skill in the Art	9
c.	Identification of the Challenge	9
i.	Claims for Which IPR is Requested	9
ii.	The Grounds on Which the Challenge is Based	9
d.	Evenhaim Grounds	10
i.	Ground 1: Obvious over Evenhaim	10
ii.	Ground 2: Obvious over Evenhaim in view of Settimi.....	34
e.	Dick Grounds	51
i.	Ground 3: Obvious over Dick in view of Landi	51
i.	Ground 4: Obvious over Dick in view of Landi and Murphy	67
7.	Conclusion	74

TABLE OF AUTHORITIES

Cases

Phillips v. AWH Corp., 415 F.3d 1303, 1313 (Fed. Cir. 2005) 7

Statutes

35 U.S.C. § 102(b) 10, 34, 51

35 U.S.C. §§ 311-319.....2

Other Authorities

37 C.F.R. § 42.100 2

37 C.F.R. § 42.100(b) 7

37 C.F.R. § 42.103(a).....2

37 C.F.R. § 42.15(a).....2

37 C.F.R. § 42.24(a).....76

37 C.F.R. § 42.24(d) 76

37 C.F.R. § 42.8(b)(1).....1

37 C.F.R. § 42.8(b)(2).....1

45 C.F.R. § 164.502(d) 25, 43

45 C.F.R. § 164.514(b) 68

45 C.F.R. § 164.514(b)(1)..... 6, 7, 27

45 C.F.R. § 164.514(b)(2).....6

45 C.F.R. § 164.514(c)(2).....6

EXHIBIT LIST

Exhibit Number	Description
1001	U.S. Patent No. 9,118,641 (the “’641 Patent”)
1002	File History of U.S. Patent No. 9,118,641
1003	Declaration of Dr. Paul Clark (“Clark”)
1004	Curriculum Vitae Of Dr. Paul Clark
1005	U.S. Pat. No. 7,823,207 (“Evenhaim”)
1006	U.S. Pat. Appl. Publ. No. 2007/0294111 (“Settimi”)
1007	U.S. Pat. Appl. Publ. No. US 2002/0111833 (“Dick”)
1008	U.S. Pat. No. 7,519,591 (“Landi”)
1009	Shawn N. Murphy and Henry C. Chueh, <i>A Security Architecture for Query Tools used to Access Large Biomedical Databases</i> , 2002 AMIA Annual Symposium Proceedings, 552 (2002) (“Murphy”)
1010	<i>Milliman, Inc. v. Gradient A.I. Corp.</i> , No. 1:21-Cv-10865-NMG (D. Mass.), Dkt. 108.
1011	<i>Credit Card Security: The Best Way to Secure Data is Not to Store the Data</i> (Hospitality Upgrade, Summer 2008, www.hospitalityupgrade.com)
1012	Jennifer G. Steiner, B. Clifford Neuman, and Jeffrey I. Schiller, <i>Kerberos: An Authentication Service for Open Network Systems</i> , Winter 1988 Usenix Conference (1988).
1013	Declaration of Sylvia Hall-Ellis, Ph.D.

CLAIM LISTING

The following claim listing adds bracketed labels ([preamble], [a]), etc.) for reference:

Representative claim 7 and its dependent claims

- [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.
- [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).

[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.

[10] The system of claim 7, in which producing the requested healthcare information includes encrypting respective data that identifies each individual.

[11] The system of claim 7, in which producing the requested healthcare information includes identifying at least a minimum number of corresponding tokens.

[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.

[13] The system of claim 7, in which the healthcare data represents medical related information associated with the individuals of the group.

Claims 1-6 and 14-19

[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.

[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).

[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.

[4] The computer-implemented method of claim 1, in which producing the requested healthcare information includes encrypting respective data that identifies each individual.

[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.

[6] The computer-implemented method of claim 1, in which the healthcare data represents medical related information associated with the individuals of the group.

[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.

[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).

[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.

[17] The computer readable storage devices of claim 14, in which producing the requested healthcare information includes encrypting respective data that identifies each individual.

[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.

[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.

1. MANDATORY NOTICES

A. REAL PARTY-IN-INTEREST UNDER 37 C.F.R. § 42.8(b)(1)

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that Datavant, Inc. and Ciox Health LLC are the real parties-in-interest.

B. RELATED MATTERS UNDER 37 C.F.R. § 42.8(b)(2)

Pursuant to 37 C.F.R. § 42.8(b)(2), U.S. Patent No. 9,118,641 is currently involved in the following proceeding: *Milliman, Inc. et al. v. Gradient AI Corp. et al.*, No. 1:21-cv-10865 (D. Mass.).

C. LEAD AND BACKUP COUNSEL AND SERVICE INFORMATION UNDER 37 C.F.R. §§ 42.8(b)(3)-(4)

Petitioner hereby designates lead and backup counsel as follows:

Lead Counsel	Backup Counsel
Peter Shapiro (Reg. No. 43,107) PShapiro@venable.com VENABLE LLP 151 W. 42nd Street, 49th Floor New York, NY 10036 T: 212-218-2201 F: 212-218-2200	Justin Oliver (Reg. No. 44,986) JOliver@Venable.com VENABLE LLP 600 Massachusetts Avenue, NW Washington, D.C. 20001 T: 202-721-5423 F: 202-344-8300 Nicholas Marcello (Reg. No. 77,182) NDMarcello@venable.com VENABLE LLP 151 W. 42nd Street, 49th Floor New York, NY 10036 T: 212-218-2365 F: 212-218-2200

	Michael Sandonato (Reg. No. 35345) MSandonato@Venable.com VENABLE LLP 2049 Century Park East, Suite 2300 Los Angeles, CA 90067 T: (310) 229-9900 F: (310) 229-9901
--	--

Petitioner consents to electronic service of documents by email at Datavant-IPRs@Venable.com.

D. PAYMENT OF FEES UNDER 37 C.F.R. §§ 42.15(a) & 42.103

The required fees are submitted herewith in accordance with 37 C.F.R. § 42.103(a) and 37 C.F.R. § 42.15(a). If additional fees are due during the proceeding, the Office is authorized to charge such fees to Deposit Account No. 22-0261. Any overpayment or refund of fees may also be deposited in this Deposit Account.

2. INTRODUCTION

Datavant, Inc. (“Petitioner”) requests *inter partes* review (“IPR”) pursuant to 35 U.S.C. §§ 311-319 and 37 C.F.R. §§ 42.100 *et seq.* of claims 1-19 (the “Challenged Claims”) of U.S. Patent No. 9,118,641 (“’641 patent”; Ex. 1001), which is assigned to Vigilytics LLC (“Patent Owner”).

The ’641 patent relates to de-identifying private healthcare data that can then be sent to third parties for their use (e.g., to insurance companies for underwriting health insurance policies). De-identification is intended to meet the requirements of

Health Insurance Portability Accountability Act (“HIPAA”) and associated regulations. De-identified information can be shared with third-parties without patient approval. Specifically, the ’641 patent states that, due to “privacy laws, companies ... are often unable to obtain [patient] health history data they need to estimate the risk of insuring [] groups.” Ex. 1001, 1:17-21, 1:30-36.

HIPAA “allows for certain entities to ‘de-identify’ protected health information so that such information may be used and disclosed freely, without being subject to the protections afforded by the Privacy Rule.” Ex. 1008, 2:5-9. “The term ‘de-identified data’ as used by HIPAA refers to patient data from which all information that could reasonably be used to identify the patient has been removed.” Ex. 1008, 2:9-12.

The ’641 patent describes de-identifying data using a “token” as an identifier. Tokenization has long been used to de-identify sensitive information regarding identity. *See* Ex. 1012; *see also* 1011, 31 (“The basics of tokenization are straightforward.... [T]he data is converted into a token which is globally unique, randomized representation of the real [information].”).

The ’641 patent claims no more than removing personally identifiable information (“PII”) from healthcare data and replacing it with a corresponding encrypted token (e.g., by using a hash). Ex. 1001, 2:37-42. Once the protected data is replaced with a token, it is no longer possible to extract PII. Ex. 1008, 2:11-55,

3:39-49. Consequently, the de-identified records can be searched for healthcare information of individuals, without their permission (and without violating HIPAA). *Id.*, 3:55-64, 4:32-35. These principles were well-known before the critical date. *Id.*, 3:65-4:3, 5:40-43.

For example, Landi describes a system for de-identifying and querying patient data by “removing the individual identifying information in the data record to generate a de-identified data record, [and] generat[ing] an encrypted ID for the individual, wherein the encrypted ID comprises an encrypted representation of one or more items of individual identifying information.” Ex. 1008, 2:44-49. “[T]he encryption system can generate de-identified data records of the individual which are associated with the encrypted ID [for the individual].” *Id.*, 3:3-5. Similarly, Evenhaim describes that PII “is replaced with a unique encryption key such as a one way hash.” Ex. 1005, 12:36-47. Thus, the prior art describes a matching token system for producing de-identified healthcare data, as claimed in the ’641 patent.

Consequently, Petitioner respectfully requests the Board institute trial.

3. GROUNDS FOR STANDING

The ’641 patent is available for IPR, and Petitioner is not barred or estopped from requesting review.

4. DISCRETIONARY DENIAL IS NOT APPROPRIATE

Discretionary denial is inappropriate here. Although the '641 patent has been asserted in a litigation, Datavant is neither a party, nor a real party-in-interest to that lawsuit.

5. OVERVIEW

A. STATE OF THE ART

Insurance companies process the health history of individuals to estimate the risk of insuring those individuals. Ex. 1001, 1:30-33; Ex. 1003, ¶34. However, this requires evaluating the health history and insurance risk, without violating federal privacy laws such as HIPAA. Ex. 1001, 1:17-23; Ex. 1003, ¶34.

HIPAA protects data in which an individual's identity is associated with their healthcare information. Ex. 1001, 1:26-28; Ex. 1005, 1:58-62; Ex. 1008, 1:58-61; Ex. 1003, ¶34. Protected information can be released if authorized by the individual; but obtaining authorization is inefficient. Ex. 1001, 1:33-36; Ex. 1008, 1:47-52; Ex. 1003, ¶34.

HIPAA allows entities to release protected health information without authorization if the healthcare information has been "de-identified." Ex. 1008, 2:5-12; Ex. 1003, ¶34. "De-identified" refers to medical records scrubbed of all information that could reasonably be used to identify the patient. Ex. 1008, 2:5-12; Ex. 1003, ¶¶34-36.

HIPAA provides two ways of implementing de-identification. The first option (“safe harbor” provision) requires removal of 18 types of information that could potentially be used to identify an individual. 45 C.F.R. § 164.514(b)(2); Ex. 1003, ¶35. However, removing that much information limits the records’ usefulness. Ex. 1003, ¶35. The second option, statistical de-identification, allows some of the fields excluded in the safe harbor provision to be included, provided there is a statistical or scientific determination that an individual’s identity cannot be reverse engineered. 45 C.F.R. § 164.514(b)(1); Ex. 1003, ¶35. Often, statistical de-identification returns a minimum number of patient records in response to a query, thereby making it impossible to associate individual health information to a specific patient. *Id.*; Ex. 1003, ¶35. In that manner, a health insurance company can review records for a specific group of individuals, without knowing which record corresponds to which individual. Ex. 1003, ¶35.

Another well-known de-identification method in the art replaces PII from a patient’s medical record with a “code,” or, in computer parlance a token, unique to each person. 45 C.F.R. § 164.514(c)(2); These tokens can then be used to query de-identified medical information without patient permission. Ex. 1005, Fig. 2, 17:27-41; Ex. 1003, ¶36.

The ’641 patent essentially claims this known method. Ex. 1003, ¶¶34-36.

6. THE '641 PATENT

The '641 patent describes de-identifying medical records using tokens. Ex. 1001, 1:14-16, 1:40-41. The tokens may be encrypted tags that replace PII in the records. The '641 patent also describes that searches preferably return a minimum number of hits, mimicking the requirement under 45 C.F.R. § 164.514(b)(1). Ex. 1001, 1:58-61; Ex. 1003, ¶34.

Independent claim 7 of the '641 patent is representative; it includes an “encryption server” for producing a token for each individual in a group, the produced token being associated with a corresponding token in a set of de-identified healthcare data. This arrangement uses the produced token to search de-identified data for relevant records. *See* claim 1. A “data server” produces requested healthcare information that characterizes the group. The identity of the individuals is unattainable from the produced information.

Claim 1 recites similar limitations in a method form, and claim 14 recites similar limitations in a computer-readable-medium form.

A. CONSTRUCTION OF THE CHALLENGED CLAIMS

The claims must be given “the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (*en banc*); 37 C.F.R. § 42.100(b).

Below are the Patent Owner's constructions from the related litigation. Ex. 1010, 9-20. Petitioner adopts these constructions for this proceeding, without waiving its right to pursue alternative constructions in any future litigation.

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

Also, regarding "token," the '641 patent states that encrypted PII is a token, which is encompassed by the foregoing construction. Ex. 1001, 1:52-54

(“Producing such a request token ... may include encrypting respective data that identifies an individual.”); Ex. 1003, ¶¶28-29.

B. PERSON OF ORDINARY SKILL IN THE ART

Petitioner submits that a 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. Superior education could compensate for less work experience, and vice-versa. Ex. 1003, ¶22.

C. IDENTIFICATION OF THE CHALLENGE

i. Claims for Which IPR is Requested

Review is requested for claims 1-19.

ii. The Grounds on Which the Challenge is Based

Ground	Claims	Basis for Unpatentability
1	1-19	Obvious over U.S. Pat. No. 7,823,207 (“Evenhaim”) (Ex. 1005)
2	1-19	Obvious over Evenhaim in view of U.S. Pat. Appl. Publ. No. US 2007/0294111 (“Settimi”) (Ex. 1006)
3	7-10 and 13	Obvious over U.S. Pat. Appl. Publ. No. US 2002/0111833 (“Dick”) (Ex. 1007) in view of U.S. Pat. No. 7,519,591 (“Landi”) (Ex. 1008)
4	1-6, 11, 12, and 14-19	Obvious over Dick in view of Landi and “A Security Architecture for Query Tools used to Access Large Biomedical Databases” by Murphy and Chueh (“Murphy”) (Ex. 1009)

The claims are unpatentable for the reasons detailed below.

D. EVENHAIM GROUNDS

i. Ground 1: Obvious over Evenhaim

Evenhaim is a U.S. patent that was published on December 6, 2007, making it prior art under at least 35 U.S.C. § 102(b) (pre-AIA).

Like the '641 patent, Evenhaim describes a protocol that allows “manipulation of privacy sensitive data while simultaneously allowing individual privacy to be preserved.” Ex. 1005, 5:4-7; Ex. 1003, ¶38. The protocol includes creating an encryption “key” token to link medical records related to an individual “without compromising the identity of that individual.” Ex. 1005, 12:12-20; Ex. 1003, ¶40. Specifically, PII “is replaced with a unique encryption key such as a one[-]way hash.” Ex. 1005, 12:4-16, 12:36-47 (“This compatible encryption for the identifying micro-level data preserves the ability to know that the two records belong to the same identity, but preserve[s] the privacy ... of that person.”). Thus, the encryption key¹ in Evenhaim is a token because it is “an identifier associated with an individual that does not reveal the identity of the individual.” Ex. 1003, ¶40.

Evenhaim describes methods that use tokens for matching de-identified patient records. Evenhaim describes loading “records from identifiable patient-

¹ The term “encryption key” in Evenhaim is used to indicate both the key used to perform encryption and the resulting encrypted information.

level micro database,” then “[d]e-identify[ing] patient information in the record using a one-way hash or other mechanism that would have the same [ID] for multiple records that belong to the same patient, yet will not allow the identification of that patient.” Ex. 1005, Figs. 1-2, 16:46-58, 17:27-41. Thus, there is a token that is used to identify all records for a specific individual. *Id.*; Ex. 1003, ¶¶39-40.

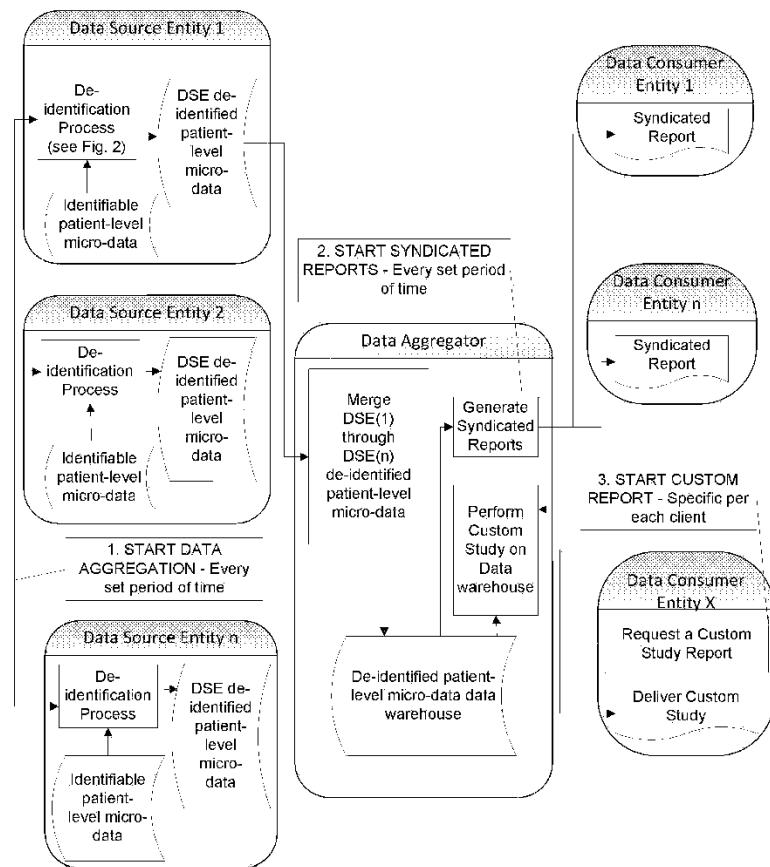


FIG. 1

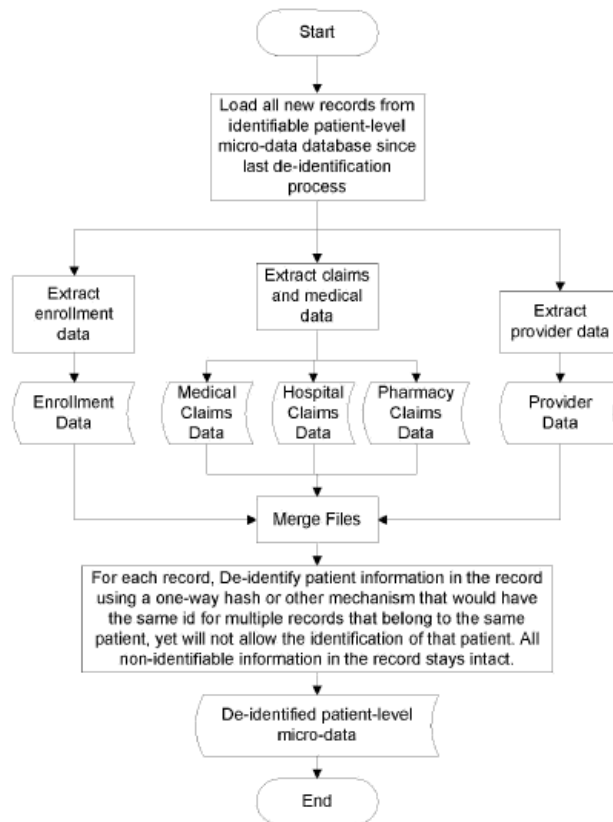


FIG. 2

Evenhaim also describes an encryption server (called a data aggregator) and at least one data server (called data sources or source entity processor), which are interconnected via a network. Ex. 1005, 6:57-63; Ex. 1003, ¶39. The data aggregator/server accepts a request for a query, which may be a list of patient names. Ex. 1005, 6:57-67, 8:18-22, Fig. 4, boxes 1-3; Ex. 1003, ¶39.

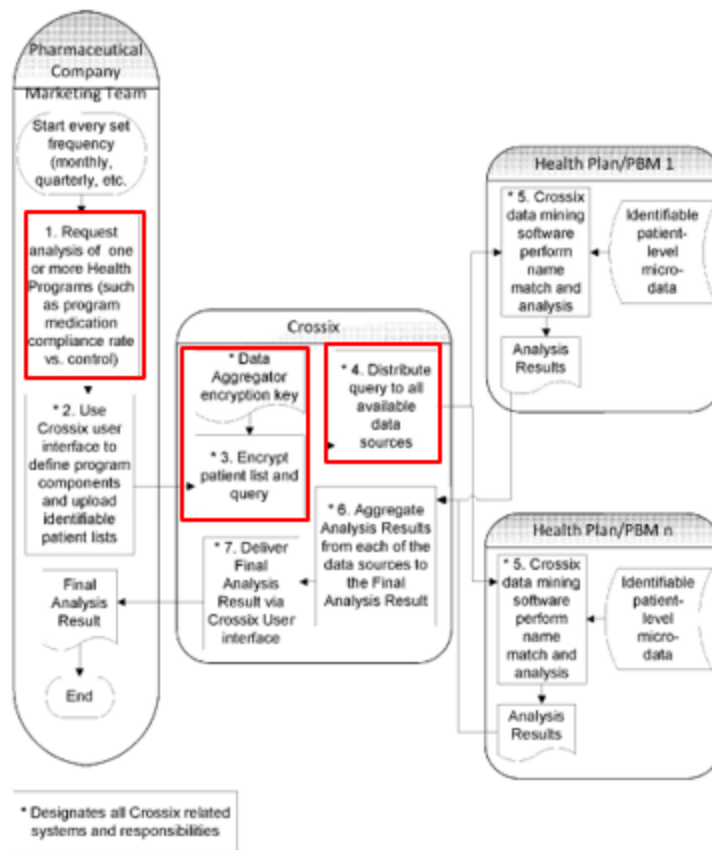


FIG. 4

Ex. 1005, 8:4-13. The aggregator encrypts the names, which a POSA would understand involves creating an encrypted token for each individual, which cannot be reversed engineered. Ex. 1003, ¶¶41, 44-45. The data sources/servers use a similar corresponding encrypted token to de-identify patient records. Ex. 1005, Fig. 4, 12:4-13:20 (“common encryption ‘key’”); Ex. 1003, ¶¶45-46. The encrypted tokens created by the aggregator for each individual are used to run queries to find corresponding encrypted tokens of the de-identified patient records. Ex. 1005, Fig. 4, 12:4-13:20; Ex. 1003, ¶¶45-46.

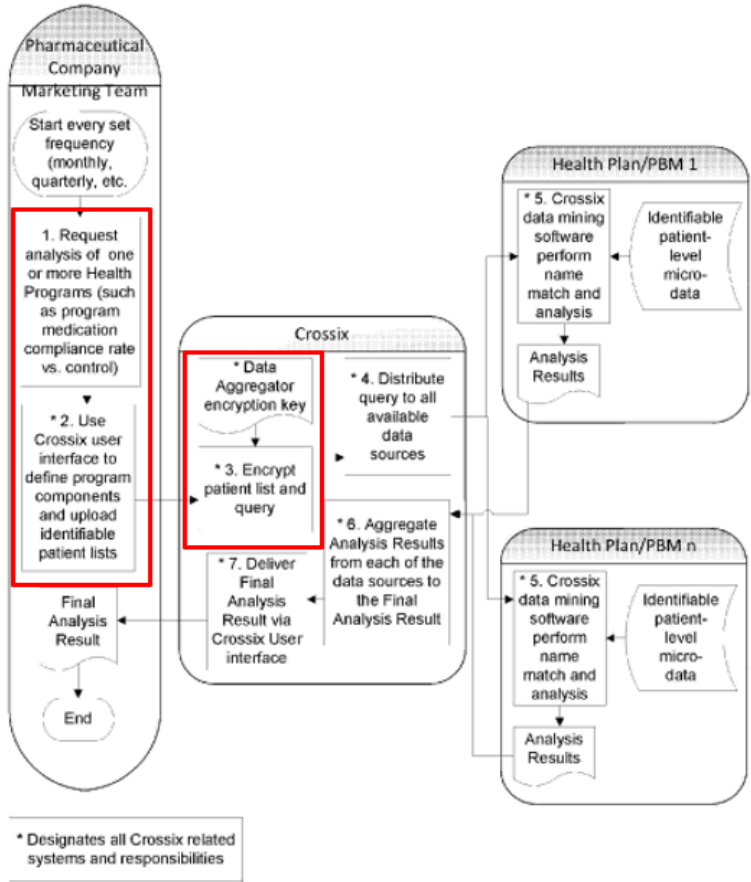
At the very least, this token matching would have been obvious in view of Evenhaim, given that token matching was well known in the field. A POSA would have understood that matching the tokens was an efficient way to query de-identified data, and would ensure compliance with HIPAA. Ex. 1003, ¶¶39-41.

Because the various servers “use a common encryption ‘key,’” the system can match patients to their medical records, even though the patient names are not known on the data server. Ex. 1005, Fig. 4, 12:4-13:20; Ex. 1003, ¶46. The data servers locate and return de-identified health information that characterizes the patients in the list. Ex. 1005, 9:29-34, 12:4-13:20, 11:31-46; Ex. 1003, ¶¶46-47.

The application of Evenhaim to representative claims 7-13, detailed below, shows that each of the Challenged Claims are obvious. Ex. 1003, ¶¶67, 133.

Claim Clause	Evenhaim Grounds
[7.a] A system comprising: an encryption server, having a processor and a memory,	Evenhaim shows an encryption server (“data aggregator”) that creates tokens, which connects with other machines using, <i>e.g.</i>, the internet. Ex. 1005, 6:34-42 (“interconnected with each other using standard data-communications facilities (e.g. Internet, VPN, etc.).”), 12:24-34 (“[T]here are numerous locations where an encryption of individual identification and/or merger of data for individuals could be facilitated..., [including] on the ‘aggregator’ processor side.”), 12:61-66 (“the personal IDs will be encrypted”), 6:57-63; Ex. 1003, ¶68. Evenhaim’s encryption server includes processor 300. Ex. 1005, 6:57-63.

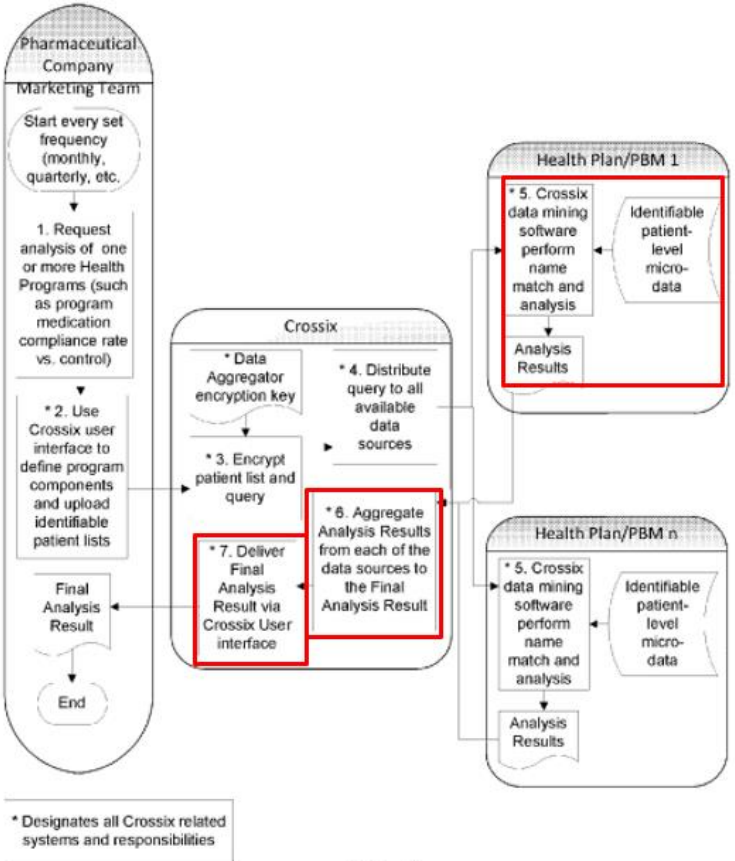
Claim Clause	Evenhaim Grounds
	A POSA would have found it obvious that the encryption server would have a memory which is routinely used to store instruction for performing functions. Ex. 1003, ¶69. Evenhaim describes software for executing the protocols is encoded in memory. <i>Id.</i>, 17:53-63 (“memory media having any of said software encoded therein”). Moreover, Evenhaim describes a standard computer system that processes and stores information to create encrypted tokens, which a POSA would understand includes a server with a processor and memory. Ex. 1005, 6:34-45, 10:64-11:2, 17:53-59; Ex. 1003, ¶69.
[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,	The data aggregator in Evenhaim produces a token (unique encryption key) for each individual in a group. Ex. 1005., Fig. 4, 12:4-13:20; Ex. 1003, ¶70. Specifically, after a request for information pertaining to a list of patients, the data aggregator applies an encryption key to encrypt those patients, which a POSA would appreciate creates tokens for each individual. Ex. 1005, Fig. 4 (steps 1-3); Ex. 1003, ¶70.

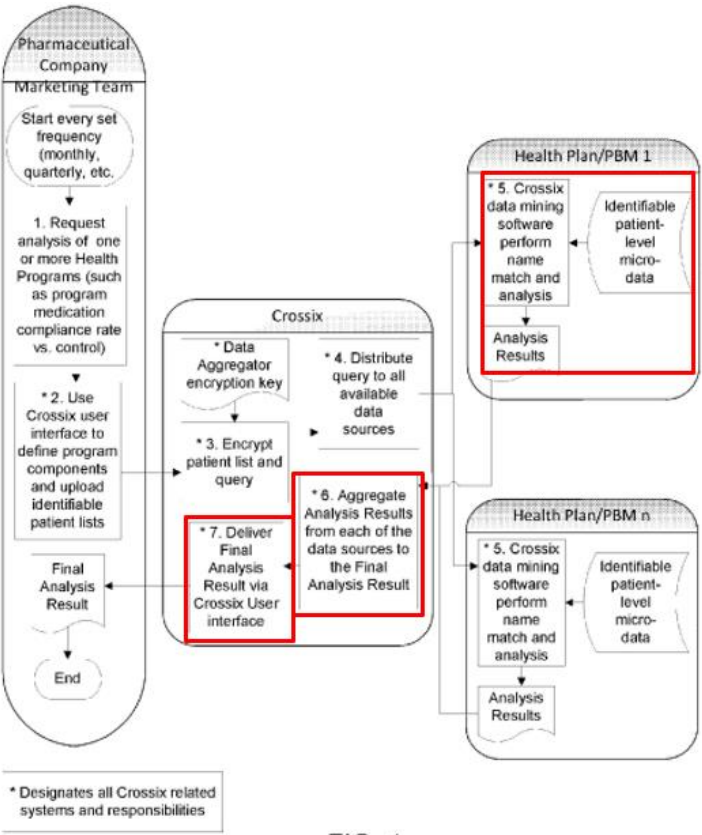
Claim Clause	Evenhaim Grounds
	 The flowchart, labeled FIG. 4, illustrates a process for analyzing health program data. It begins with a 'Pharmaceutical Company Marketing Team' box, which includes a note 'Start every set frequency (monthly, quarterly, etc.)'. An arrow points down to a box containing two steps: '1. Request analysis of one or more Health Programs (such as program medication compliance rate vs. control)' and '* 2. Use Crossix user interface to define program components and upload identifiable patient lists'. This box is highlighted with a red border. An arrow points down to a 'Final Analysis Result' box, which then leads to an 'End' box. To the right, a 'Crossix' box contains several steps: '* Data Aggregator encryption key', '* 3. Encrypt patient list and query' (highlighted with a red border), '* 4. Distribute query to all available data sources', '* 6. Aggregate Analysis Results from each of the data sources to the Final Analysis Result', and '* 7. Deliver Final Analysis Result via Crossix User interface'. Arrows connect the 'Crossix' box to two 'Health Plan/PBM' boxes (labeled 'Health Plan/PBM 1' and 'Health Plan/PBM n'). Each 'Health Plan/PBM' box contains a step: '* 5. Crossix data mining software perform name match and analysis' and 'Identifiable patient-level micro-data'. Arrows point from these boxes to 'Analysis Results' boxes, which then feed into the 'Crossix' box's step 6. A legend at the bottom left states: '* Designates all Crossix related systems and responsibilities'. FIG. 4 In particular, “the instant method can ask about the status of Tom, Dick, Harry, and a further collection of individuals—and obtain results from that query.” Ex. 1005, 8:18-22, 6:64-67, 8:4-13 (“the parameters of the list may include identity disclosing specific ... such things as name, personal identity number or simple data combinations”); Ex. 1003, ¶70. The request is for healthcare information that characterizes the group, including the de-identified patient records themselves, identifying common treating physicians, and tracking outcomes of patients in a clinical trial. Ex. 1005, Fig. 5, 7:12-26, 8:65-9:12, 15:3-14, 15:25-45.

Claim Clause	Evenhaim Grounds
	At the very least, a POSA would understand that the token creation and matching system described in Evenhaim could be applied to the embodiment in Fig. 4 and 4A such that the aggregator would create encrypted tokens from the list of patients received in Fig. 4, box 3 in order to create the query to the data sources in box 4, and get de-identified patient data back from the data sources in box 6. <i>Id.</i>, 12:4-13:20; Ex. 1003, ¶¶72-74. The specification explains that the token creation could be performed on the aggregator as well as at the data sources. Ex. 1005, 12:24-34; Ex. 1003, ¶70. Token creation and matching have been in common use since the 1980’s. <i>Id.</i>, ¶71; Ex. 1012.
[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,	Evenhaim explains that the identity of the individuals is unattainable from the tokens. Evenhaim uses, e.g., a one-way hash that creates the tokens from PII, which preserves the privacy of the patient by eliminating the PII, but still allows linking records for the same person. Ex. 1005, 12:38-45 (“[T]he person[al] identity information, for the matched population, is replaced with a unique encryption key, such as a one way hash or Advanced Encryption Standard (AES) or the like[.]. This compatible encryption ... preserves the ability to know that the two records belong to the same identity, but preserve the privacy of the identity of that person.”), 8:18-22 (“will not allow correlation of a result specific back to an individual.”); Ex. 1003, ¶75. Even when two-way encryption is used, the identity of the individuals is not obtainable from the tokens absent the decryption key, which Evenhaim explains would not be available to the entity linking the records to match the patients. Ex. 1005, 12:16-20; Ex. 1003, ¶75. A POSA would have understood that each token produced for the group corresponds to tokens used on the data servers to de-identify patient records, in that

Claim Clause	Evenhaim Grounds
	Evenhaim describes common encryption across servers for identifying multiple records for the same individual through the corresponding tokens. Ex. 1005, (“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.”), 12:36-67, 13:1-20; Ex. 1003, ¶¶75-76. At the very least, it would be obvious to a POSA to implement the system so each token generated by the aggregator is associated with a token in the data sources that was generated to de-identify the patient records. Indeed, Fig. 4 shows that encryption occurs on the aggregator side to produce tokens sent to the data sources to obtain corresponding patient data. Ex. 1003, ¶77. Thus, a POSA would understand that the tokens produced by the aggregator from the list of individuals in the query, correspond to tokens that are inserted into the patient records on the data source. <i>Id.</i>
[7.d] and each token in the set of de-identified healthcare data being associated with healthcare data for a corresponding individual;	As addressed above, Evenhaim explains that each token is de-identified personal data associated with that individual’s healthcare records. Ex. 1003, ¶78. Specifically, “the data sources are careful to encrypt the identifying portions of each record using a common encryption ‘key’” such that each individual’s healthcare record is de-identified with the token. Ex. 1005, 12:8-16, 12:38-45 (“[T]he person identity information, for the matched population, is replaced with a unique encryption key This ... preserves the ability to know that the two records belong to the same identity”); Ex. 1003, ¶78. Figs. 4, and 4A show how the tokens are associated with patient records. <i>See</i> Ex. 1005, 12:4-13:20. In box 5, the

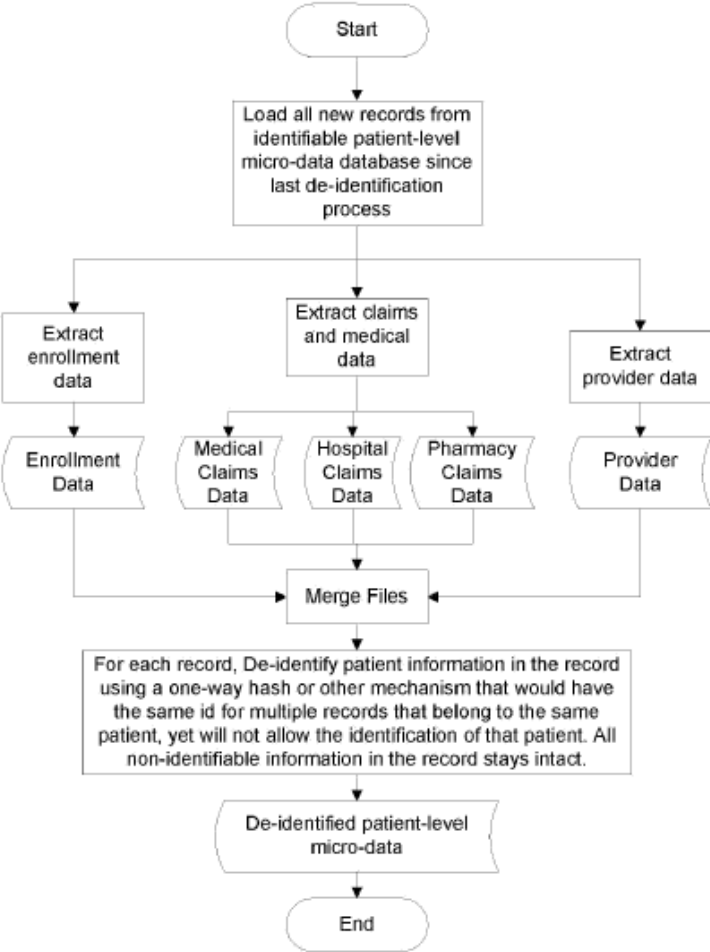
Claim Clause	Evenhaim Grounds
	data source matches the tokens against the de-identified records to find the ones responsive to the query (called patient-level micro-data). Further, Evenhaim explains it was known that patient records may be de-identified prior to searching. <i>Id.</i>, 17:27-40. Thus, it was obvious to a POSA that de-identification of records could take place before or after receiving the search request. Ex. 1003, ¶¶79-80.
[7.e] a data server for producing the requested healthcare information that characterizes the group	Evenhaim describes a data server called a “data source,” “source entity” or “data source entity” for producing the requested healthcare information that characterizes the group. The source entity is a computer processor having software that allows it to execute its protocol, and memory such as optical disks, read only memory and the like. Ex. 1005, 17:53-63, 5:12-28; Ex. 1003, ¶¶81-83. The data source receives requests from the encryption server (data aggregator) and responds to those requests by producing the healthcare information that characterizes the group, including the de-identified records. Ex. 1005, Figs. 4, 4A, 5, 12:13-16, 12:42-45; Ex. 1003, ¶¶81-83. The data sources provide various types of health information that characterizes the group, including the de-identified patient records for listed patients, treating physicians, health outcomes, etc. Ex. 1005, 8:65-9:12, 15:3-14, 15:25-45, 8:49-64 (“the aggregator receives some answer (or a null answer) from each source-entity”), 6:63-7:27; Ex. 1003, ¶84. Ex. 1005, Fig. 4 (showing results from searching for information at the data source (Health Plan/PBM) are provided to the aggregator).

Claim Clause	Evenhaim Grounds
	 FIG. 4 * Designates all Crossix related systems and responsibilities
[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,	As discussed, Evenhaim describes tokens in the form of unique encryption keys created from PII using a one-way hash. Ex. 1005, 12:38-42, 8:18-22, 6:64-67, 8:4-13, 12:27-33 (“[T]here are numerous locations where encryption of individual identification... could be facilitated.”); Ex. 1003, ¶85. Figs. 4 and 4A show how the produced tokens from the aggregator are sent to the data server (see boxes 3-5). It would be obvious that, at the data server, in box 5, the data source matches the query information against the de-identified patient records, which may occur by matching the produced tokens to corresponding tokens in a set of de-identified patient records. Ex. 1005, 12:4-47 (explaining that the encryption key is used on the data

Claim Clause	Evenhaim Grounds
	server side to de-identify the records), 17:27-40 (explaining that tokenization may occur before searching); Ex. 1003, ¶85. Thus, in Evenhaim tokens sent from the aggregator are matched against the tokens in the de-identified patient records in the data sources to retrieve the de-identified patient data. Ex. 1005, 12:13-16, 12:42-45. Fig. 4, box 4, shows a query sent to the data sources, which perform matching in box 5 then return the results to the aggregator in box 6.  <pre> graph TD subgraph PC [Pharmaceutical Company Marketing Team] Start([Start every set frequency (monthly, quarterly, etc.)]) Step1[1. Request analysis of one or more Health Programs (such as program medication compliance rate vs. control)] Step2[2. Use Crossix user interface to define program components and upload identifiable patient lists] FinalResult[Final Analysis Result] End([End]) Start --> Step1 Step1 --> Step2 Step2 --> FinalResult FinalResult --> End end subgraph Crossix Key[Data Aggregator encryption key] Step3[3. Encrypt patient list and query] Step4[4. Distribute query to all available data sources] Step6[6. Aggregate Analysis Results from each of the data sources to the Final Analysis Result] Step7[7. Deliver Final Analysis Result via Crossix User interface] Key --> Step3 Step3 --> Step4 Step4 --> Step6 Step6 --> Step7 Step7 --> FinalResult end subgraph HP1 [Health Plan/PBM 1] Step5_1[5. Crossix data mining software perform name match and analysis] ID1[Identifiable patient-level micro-data] Results1[Analysis Results] ID1 --> Step5_1 Step5_1 --> Results1 end subgraph HPn [Health Plan/PBM n] Step5_n[5. Crossix data mining software perform name match and analysis] IDn[Identifiable patient-level micro-data] Resultsn[Analysis Results] IDn --> Step5_n Step5_n --> Resultsn end Step4 --> HP1 Step4 --> HPn Results1 --> Step6 Resultsn --> Step6 </pre> * Designates all Crossix related systems and responsibilities

At the very least, a POSA would understand that the token creation and matching in Evenhaim could be applied to the embodiment in Fig. 4 and 4A such that the data sources in box 6 would have de-identified records with encrypted tokens that are identified in response to a query to the data sources sent in box 4. The specification

Claim Clause	Evenhaim Grounds
	teaches that the token creation could be performed on the aggregator as well as on the data sources. Ex. 1005, 12:26-34; Ex. 1003, ¶¶84-86. This can also be seen in the system disclosed in Figs. 1-2 showing the prior art in which de-identified records are associated with a one-way hash that can be queried to create a report. Ex. 1005, 16:46-58, 17:27-41; Ex. 1003, ¶¶86-87. <pre> graph TD subgraph DS_Entities [Data Source Entities] DSE1[Data Source Entity 1] DSE2[Data Source Entity 2] DSEn[Data Source Entity n] end subgraph DA [Data Aggregator] Merge[Merge DSE(1) through DSE(n) de-identified patient-level micro-data] Warehouse[(De-identified patient-level micro-data data warehouse)] Generate[Generate Syndicated Reports] Custom[Perform Custom Study on Data warehouse] end subgraph DC_Entities [Data Consumers] DC1[Data Consumer Entity 1] DCn[Data Consumer Entity n] DCX[Data Consumer Entity X] end DSE1 -- "Identifiable patient-level micro-data" --> DSE1_DeID[De-identification Process] DSE1_DeID -- "DSE de-identified patient-level micro-data" --> DA_Warehouse DSE2 -- "Identifiable patient-level micro-data" --> DSE2_DeID[De-identification Process] DSE2_DeID -- "DSE de-identified patient-level micro-data" --> DA_Warehouse DSEn -- "Identifiable patient-level micro-data" --> DSEn_DeID[De-identification Process] DSEn_DeID -- "DSE de-identified patient-level micro-data" --> DA_Warehouse DA_Warehouse -- "2. START SYNDICATED REPORTS - Every set period of time" --> DA_Generate[Generate Syndicated Reports] DA_Generate --> DC1_Syn[Syndicated Report] DA_Generate --> DCn_Syn[Syndicated Report] DCX -- "3. START CUSTOM REPORT - Specific per each client" --> DCX_Request[Request a Custom Study Report] DCX_Request --> DA_Custom[Perform Custom Study on Data warehouse] DA_Custom --> DCX_Deliver[Deliver Custom Study] </pre> The diagram illustrates a data processing system. On the left, multiple 'Data Source Entity' boxes (1, 2, n) each contain a 'De-identification Process' (referencing Fig. 2) and a 'DSE de-identified patient-level micro-data' output. These entities feed 'Identifiable patient-level micro-data' into their respective de-identification processes. The output of these processes is 'DSE de-identified patient-level micro-data', which is then sent to a central 'Data Aggregator'. The aggregator performs a 'Merge DSE(1) through DSE(n) de-identified patient-level micro-data' and stores it in a 'De-identified patient-level micro-data data warehouse'. From the warehouse, the system can generate 'Syndicated Reports' (labeled '2. START SYNDICATED REPORTS - Every set period of time') which are then sent to 'Data Consumer Entity 1' and 'Data Consumer Entity n'. Alternatively, a 'Data Consumer Entity X' can 'Request a Custom Study Report' (labeled '3. START CUSTOM REPORT - Specific per each client'), which is then processed by the aggregator's 'Perform Custom Study on Data warehouse' component and finally 'Deliver Custom Study' to the consumer. FIG. 1

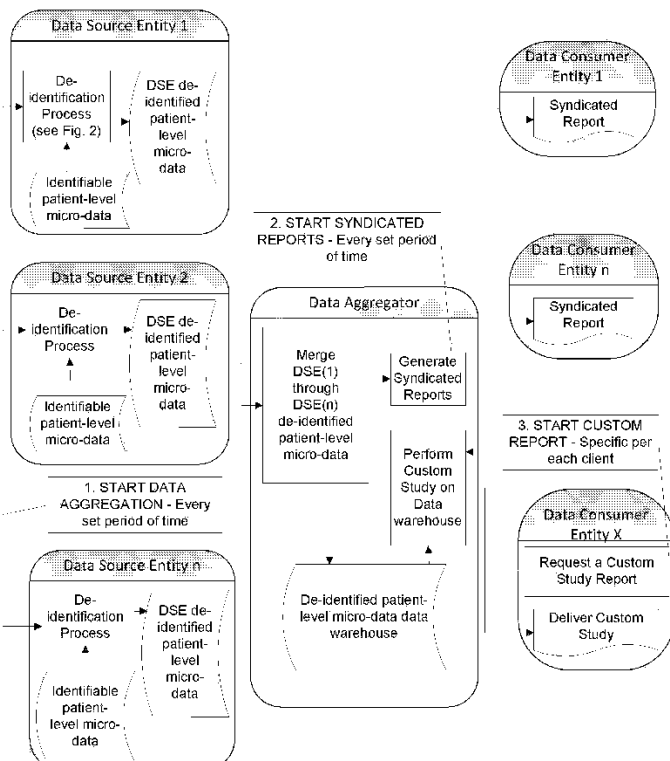
Claim Clause	Evenhaim Grounds
	 <pre> graph TD Start([Start]) --> Load[Load all new records from identifiable patient-level micro-data database since last de-identification process] Load --> ExtractEnroll[Extract enrollment data] Load --> ExtractClaims[Extract claims and medical data] Load --> ExtractProvider[Extract provider data] ExtractEnroll --> EnrollData[/Enrollment Data/] ExtractClaims --> MedicalClaims[/Medical Claims Data/] ExtractClaims --> HospitalClaims[/Hospital Claims Data/] ExtractClaims --> PharmacyClaims[/Pharmacy Claims Data/] ExtractProvider --> ProviderData[/Provider Data/] EnrollData --> MergeFiles[Merge Files] MedicalClaims --> MergeFiles HospitalClaims --> MergeFiles PharmacyClaims --> MergeFiles ProviderData --> MergeFiles MergeFiles --> DeIdentify[For each record, De-identify patient information in the record using a one-way hash or other mechanism that would have the same id for multiple records that belong to the same patient, yet will not allow the identification of that patient. All non-identifiable information in the record stays intact.] DeIdentify --> DeIdentifiedData[/De-identified patient-level micro-data/] DeIdentifiedData --> End([End]) </pre> FIG. 2 Evenhaim discloses some embodiments for producing healthcare information that do not match tokens. In some of those embodiments, de-identification takes place after the records are matched. Ex. 1005, Fig. 5, 17:42-52. A POSA would, however, understand that for embodiments that apply tokens on the encryption server side, as discussed herein and shown in Fig. 4, to replace PII, where records on the data source side are also de-identified through tokenization, then relevant records could be located by matching tokens instead of patient names. Ex. 1003, ¶¶39, 86. In fact, Evenhaim calls for

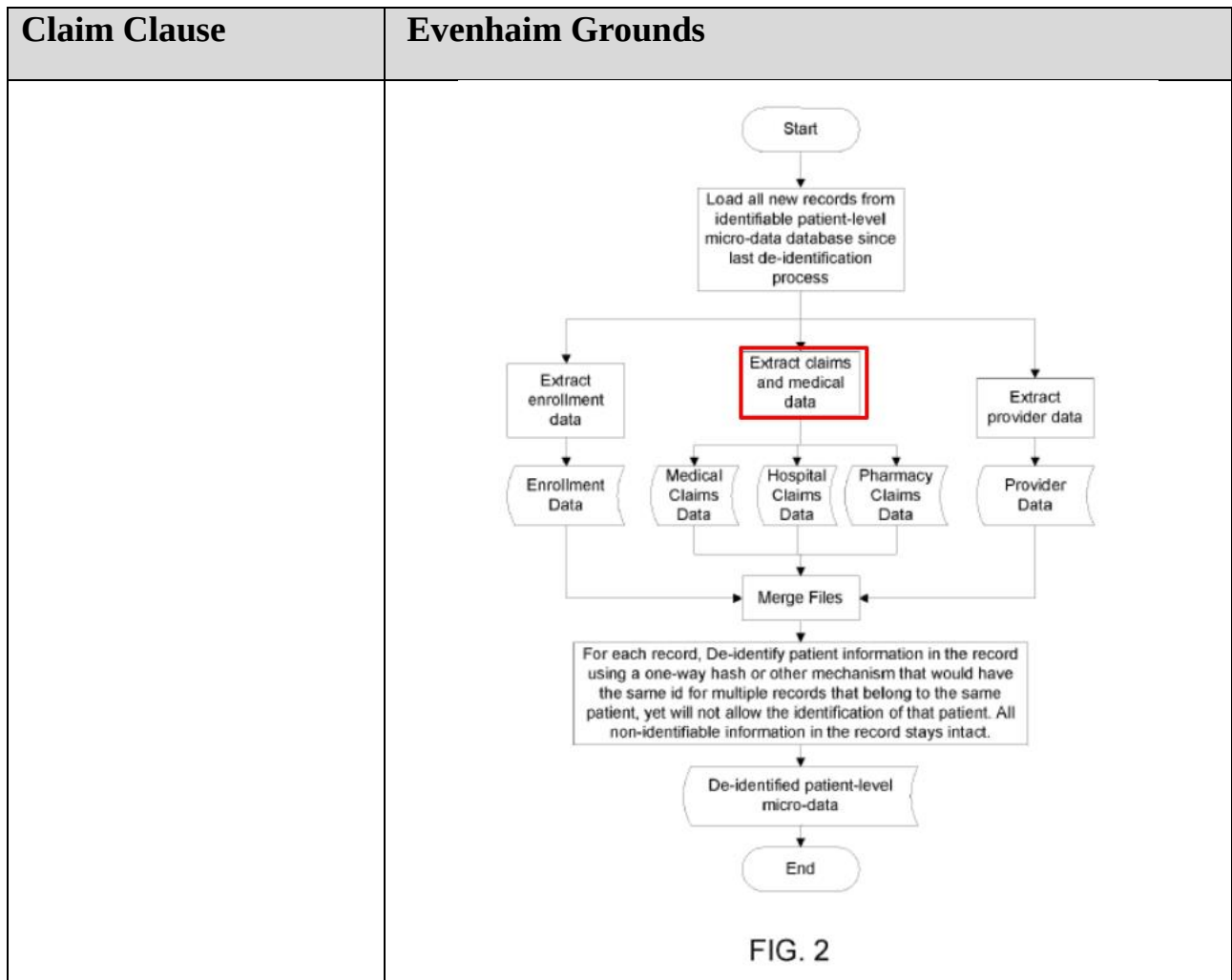
Claim Clause	Evenhaim Grounds
	“using a common encryption ‘key’” in order to match records. Ex. 1005, 12:4-16; 12:27-33 (“[T]here are numerous locations where an encryption of individual identification ... could be facilitated. By way of non-limiting example, on the ‘aggregator’ processor side ... or on the ‘source-entity’ processors’ side”). Thus, a POSA applying these features to the embodiment of Fig. 4 would logically have produced tokens created from the parameter list received by the data aggregator (box 3), using the common encryption key, for the query. In this manner, the tokens could be matched to corresponding tokens on the data source side using the same encryption key, with the matching records being returned to the aggregator in box 6. <i>Id.</i>, 12:37-41; Ex. 1003, ¶86. This would allow for both locating the relevant records and ensuring that multiple records from the same patient can be matched together, even after de-identification. Ex. 1005, 12:49-52 (“[T]he ability to link micro-level records related to the same identity at the data aggregator level is preserved – even if the records came from two different data sources.”). Otherwise, the operation shown in Fig. 4 would require encryption of the patient names on the encryption server side, sending of the query to a data source, decrypting the names in order to perform name matching, and then de-identifying the located record using encryption in order to send the results to the encryption server side. Ex. 1003, ¶86. Of course, additional encryption could be used before sending the results to the encryption server to further ensure privacy. <i>Id.</i>, ¶42.
[7.g] wherein the produced tokens and the tokens in the set of de-	Evenhaim explains that the produced tokens from the aggregator and tokens in the de-identified data on the data sources are similarly encrypted. Ex. 1005, 12:39-44 (“compatible encryption”), 12:4-16 (“common

Claim Clause	Evenhaim Grounds
identified data are similarly encrypted,	encryption ‘key’”). Common encryption is used, at least, in order to ensure that records for the same patient can be matched. <i>Id.</i> , 12:12-16 (“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 identify of that individual.”), 12:25-30, 16:46-57, 17:27-41; Ex. 1003, ¶¶88-89.
[7.h] and the produced healthcare information is absent personally identifiable information	The produced healthcare information is absent PII because the data is de-identified. Ex. 1005, 9:13-18 (“de-identified data collection.”), 8:49-64, 10:1-6, 12:12-20, 12:35-44, 14:8-13; Ex. 1003, ¶¶90-91.
[7.i] and has been produced without the individuals in the group having authorized production of such healthcare information that characterizes the group; and	A purpose of Evenhaim is to produce de-identified healthcare information that can be released to third-parties without individuals in the group authorizing the release, to comply with HIPAA. Ex. 1005, 3:17-31, 4:34-48, 5:46-6:10, 8:18-22, 14:7-13, 15:15-24, 14:59-67, 3:26-31; Ex. 1003, ¶92. Per HIPAA, the purpose of de-identification is to create shareable data that does not require permission from each included patient. HIPAA, 45 C.F.R. § 164.502(d), 164.508; Ex. 1001, 1:33-36, 4:1-3. Otherwise, there is no need to de-identify the healthcare information. Ex. 1003, ¶92.
[7.j] providing the produced healthcare information to report the characteristics of the group composed of multiple individuals	The produced healthcare information reports the characteristics (the medical information) of the group. Ex. 1005, Fig. 4 (<i>see</i> boxes 6 and 7), 10:6-11(“[T]he aggregator may now collect and assemble identity protected reports from numerous data collections (source-entities) and assemble them into a single report.”), 15:3-14; Ex. 1003, ¶93; <i>see</i> 7.b and 7.d above.

Claim Clause	Evenhaim Grounds
	Various types of health information that characterizes the group are provided, including the de-identified patient records themselves. Ex. 1005, Fig. 5, 7:12-26, 8:65-9:12, 15:3-14, 15:25-45; Ex. 1003, ¶93.
[7.k] absent authorization at any time from the individuals in the group of individuals to provide the requested healthcare information.	Evenhaim provides the healthcare information without authorization “at any time” from the individuals because it describes de-identification for that purpose under HIPAA. <i>See</i> 7.i above; Ex. 1003, ¶94.
[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).	Evenhaim describes producing healthcare information absent authorization in accordance with HIPAA. <i>See</i> 7.i above. As also discussed above (7.i), a POSA would find this limitation is obvious where Evenhaim is directed to de-identifying health information to comply with HIPAA. Ex. 1003, ¶55.
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.	Evenhaim describes that the request may include a “parameter list,” which may include names, dates of birth, etc. Ex. 1005, 13:62-14:13, 8:39-43 (“parameter list may even include specific individuals by name or ID or the like[.]”), 8:18-22 (“For example, the instant method can ask about the status of Tom, Dick, Harry ...”), 12:38-45, 12:8-16; Ex. 1003, ¶96.
10. The system of claim 7, in which producing the requested healthcare	As discussed above with respect to claim 7, Evenhaim produces healthcare information in which the PII has been encrypted. Ex. 1005, 12:4-20 (“encrypt the

Claim Clause	Evenhaim Grounds
information includes encrypting respective data that identifies each individual.	identifying portions of each record”), 12:24-34 (“encryption of individual identification”), 8:39-48, 12:4-67, 13:1-12, Figs. 1, 2, 4A, 5; Ex. 1003, ¶¶97-99.
11. The system of claim 7, in which producing the requested healthcare information includes identifying at least a minimum number of corresponding tokens.	Evenhaim describes “the inclusion of at least a predetermined minimum number of individuals.” Ex. 1005, 13:62-65; Ex. 1003, ¶100. A POSA would understand that requiring a minimum number of individuals corresponds to having a minimum number of tokens used in processing the query because the tokens correspond to individuals. Ex. 1003, ¶100. The number of individuals must be sufficient to protect privacy. Ex. 1005, 8:13-48 (“It will simply be necessary that the number of the individuals in any population definition be large enough to dilute any definitive conclusion about an individual’s personal data.”), 16:5-32; Ex. 1003, ¶101. This concept is required by the HIPAA Expert Determination method, with which Evenhaim is intended to comply. 45 C.F.R. § 164.514(b)(1).
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.	See claim 11 above; Ex. 1003, ¶102.
13. The system of claim 7, in which the healthcare data represents medical related information associated with the individuals of the group.	Evenhaim’s data represents medical related information associated with the individuals of the group, which it sometimes refers to as micro-data or patient-level micro-data. Ex. 1005, Abstract, Figs. 1, 2, 5; 10:46-54, 11:14-29, 12:36-47; Ex. 1003, ¶¶27, 103. Also, Figs. 1 and 2 show a de-identification system where the healthcare data represents medical related

Claim Clause	Evenhaim Grounds
	information associated with the individuals of the group. Ex. 1005, 16:46-57, 17:27-41; Ex. 1003, ¶¶27, 103.  FIG. 1



Claim Clause	Evenhaim Grounds
[1.a] A computer-implemented method comprising: receiving a request for healthcare information that characterizes a group ..., the healthcare information being assembled from healthcare data that comprises de-identified information;	See 7.a, 7.b, 9 above.

Claim Clause	Evenhaim Grounds
[1.b] producing, by a processor of an encryption server, tokens,	See 7.a, 7.b above.
[1.c] wherein the identity of the individuals ... is unattainable from the tokens, each token being associated with an individual ..., each token being associated with a corresponding token in a set of de-identified healthcare data, and	See 7.c above.
[1.d] each token ... being associated with healthcare data for a corresponding individual;	See 7.d above.
[1.e] when the group includes at least a minimum number of individuals,	See 11 above.
[1.f] producing the requested healthcare information that characterizes the group by identifying the tokens ... and ... de-identified healthcare data ...,	See 7.f, 7.h above.
[1.g] wherein the ... tokens ... are similarly encrypted, and	See 7.g, 7.i above.
[1.h] ... information is absent personally	See 7.j above.

Claim Clause	Evenhaim Grounds
identifiable information and	
[1.i] has been produced without the individuals ... having authorized production ...; and	See 7.k above.
[1.j] providing the produced healthcare information	See 7.b, 7.j, 7.k above.
[2] The computer-implemented method of claim 1, wherein the healthcare information ... is in conformity with ... (HIPAA).	See 8 above.
[3] The computer-implemented method of claim 1, ... receiving personally identifiable information associated with members of the group	See 9 above.
[4] The computer-implemented method of claim 1, in which producing the requested healthcare information includes encrypting	See 10 above.
[5] The computer-implemented method of claim 1, in which producing the requested healthcare information includes identifying at least a minimum number	See 11 above.
[6] The computer-implemented method of	See 13 above.

Claim Clause	Evenhaim Grounds
claim 1, in which the healthcare data represents medical related information	
[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:	See 7.a above.
[14.b] receiving a request for healthcare information that characterizes a group ..., the healthcare information being assembled from ... de-identified information;	See 7.b above.
[14.c] producing, by a processor of an encryption server, tokens,	See 7.a, 7.b, 7.f above.
[14.d] wherein the identity of the individuals in the group is unattainable ...;	See 7.c, 7.d above.
[14.e] when the group includes ... a minimum number of individuals,	See 11 above.
[14.f] producing the requested healthcare information ... by	See 7.f above.

Claim Clause	Evenhaim Grounds
identifying the tokens ...,	
[14.g] wherein the ... tokens ... are similarly encrypted, and	See 7.g above.
[14.h] the produced healthcare information is absent personally identifiable information ...; and	See 7.i above.
[14.i] providing the produced healthcare information to report the characteristics of the group ... absent authorization	See 7.j above.
[15] The computer readable storage devices of claim 14, wherein the healthcare information provided ... is in conformity with ... (HIPAA).	See 7.i above.
[16] The computer readable storage devices of claim 14, wherein the request for healthcare information ... includes personally identifiable information	See 9 above.
[17] The computer readable storage devices of claim 14, in which producing the requested healthcare information includes encrypting	See 10 above.
[18] The computer readable storage devices	See 11 above.

Claim Clause	Evenhaim Grounds
of claim 14, ... identifying at least a minimum number of corresponding tokens.	
[19] The computer readable storage devices of claim 14, in which the healthcare data represents medical related information	See 13 above.

ii. Ground 2: Obvious over Evenhaim in view of Settimi

Evenhaim in view of Settimi further establishes that claims 1-19 are unpatentable. Ex. 1003, ¶134.

Settimi is a U.S. patent application that published on Dec. 20, 2007, and is prior art under at least 35 U.S.C. § 102(b) (pre-AIA); Ex. 1003, ¶49.

Settimi relates to de-identifying patient data, in compliance with HIPAA, using encrypted tokens and making the de-identified patient data available in a central repository. Ex. 1006, Figs. 1-3, [0027], [0030], [0035]-[0043], [0047]-[0048], claim 5; Ex. 1003, ¶50. Specifically, Settimi describes a centralized warehouse of de-identified patient records, collected from various patient care providers. Ex. 1006, Fig. 2, [0027]; Ex. 1003, ¶50. This central repository allows the patient data to be queried for, e.g., research, while keeping the centralized records HIPAA compliant. Ex. 1006, [0027], [0030], [0035] (“The de-identified

patient data is then staged into a data warehouse 210 where it is available for querying.”), [0036]; Ex. 1003, ¶50.

To de-identify the data, Settimi generates encrypted tokens for individuals, called encoded patient identifiers, or EPIDs, which may be encoded versions of PII. Ex. 1006, [0041]-[0042] (“the EPID ... may be [based on] patient name, age and social security number, etc.”); Ex. 1003, ¶51. The EPIDs replace the PII to create the de-identified patient records in the repository. Ex. 1006, [0038]-[0041], [0043] (“The de-identified patient data includes an EPID 308 that may be useful in creating longitudinal reports that analyze more than one record for a particular patient.”); Ex. 1003, ¶51.

Once de-identified and stored in the central repository, the healthcare records can be queried using a token matching scheme. 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. Ex. 1006, [0037] (“[C]reat[ing] patient cohort reports 212 based on the querying the longitudinal patient data is supported by the ability to connect all records relating to a single patient in the data warehouse 210. This requires a unique identifier to be associated with each patient record that is transmitted to the data warehouse 210. The unique identifier indicates an ... abstract patient having certain characteristics but does not provide personal direct identifying information.”); Ex. 1003, ¶52. In

this regard, Settimi's central repository overcomes prior central repository designs that do not allow for the identification of individual patients, which is Evenhaim's stated goal. Ex. 1005, 16:46-67; Ex. 1003, ¶48. As would have been appreciated by a POSA, these queries could be used for various purposes. Ex. 1006, [0043]; Ex. 1003, ¶¶52, 134-35. Advantageously, the searches are performed in a central repository with records gathered from across institutions, which records are stripped of PII before being sent to the central repository.

Both Evenhaim and Settimi seek to provide access to patient data in a manner that complies with privacy regulations and provides sufficient information for statistical analysis. Ex. 1003, ¶¶47, 51, 135. While Evenhaim sends healthcare data queries to various healthcare organizations, Settimi consolidates the information from the various providers in a central repository for queries. See Ex. 1005, 15:15-24, 16:5-21, Fig. 4; Ex. 1006, Figs. 1-2, [0027]; Ex. 1003, ¶137. The repository eliminates the need for conducting searches across different entities and uses a "common vocabulary" that makes searching easier and more reliable. Ex. 1006, [0009], [0060]-[0062]; Ex. 1003, ¶136.

Thus, a POSA would have appreciated that using Settimi's central repository for storing de-identified records, and using a common vocabulary, allows for a single query, to a single repository, using standardized search vocabulary, while still allowing for searches for specific patients. Ex. 1006, [0060]; Ex. 1003, ¶135-

36. Also, per Settimi, the central repository/warehouse for searching contains only de-identified healthcare records, reducing the risk of a HIPAA violation. For these reasons, a POSA would be motivated to combine the centralized warehouse concept in Settimi with Evenhaim. Ex. 1003, ¶¶135-38.

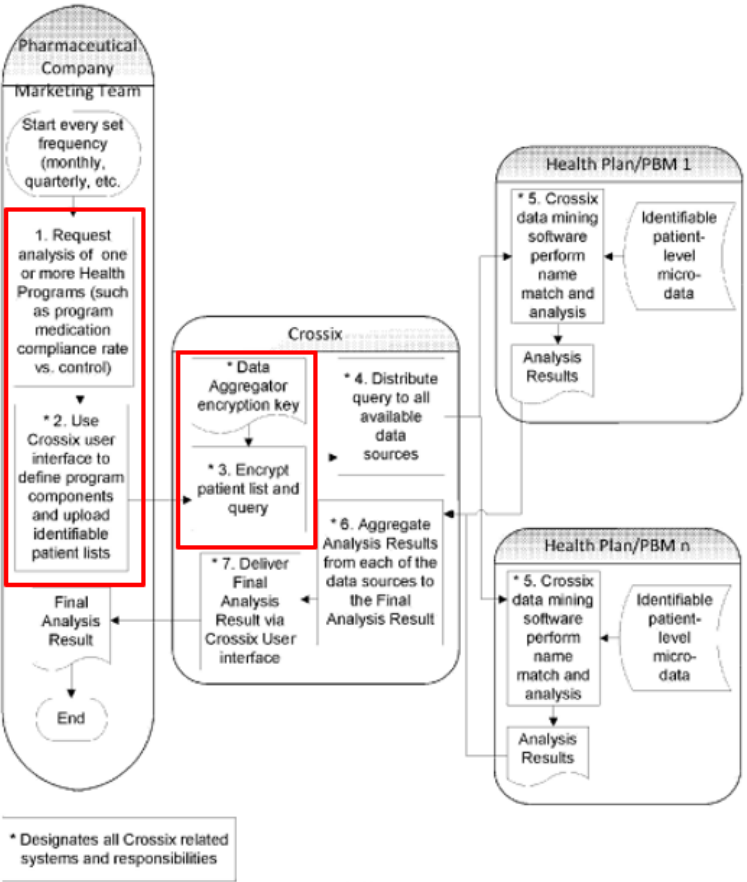
A POSA would have a reasonable expectation of success in combining Evenhaim and Settimi because they are both performed in similar environments and involve de-identifying patient data so that it may be analyzed by third parties. *Id.*, ¶138. Indeed, the combination would essentially involve simply changing the database system in which records are stored. *Id.*

Thus, a POSA would have been motivated to combine Evenhaim's de-identification system in Figs. 4 and 4A with Settimi's centralized warehouse to simplify querying, ensure no healthcare information is missing from the query results, further protect patient privacy, and allow for standardized search terms. Ex. 1006, [0009], [0014], [0017], [0027], [0039]-[0040]; Ex. 1003, ¶¶135-138.

The claim chart below shows that each of the Challenged Claims are obvious over Evenhaim in view of Settimi.

Claim Clause	Evenhaim in view of Settimi Ground
[7.a] A system comprising: an encryption server, having a processor and a memory,	See 7.a (Ground 1) above.

Claim Clause	Evenhaim in view of Settimi Ground
[7.b] for producing a token for each individual included in a group ... identified in a request for healthcare information that characterizes the group,	Evenhaim shows this feature for the reasons discussed above. See 7.b (Ground 1) above. In particular, tokens are created in step 3 in Fig. 4, prior to the query being sent to the repository. With the combination, the query would be prepared to be sent to a central warehouse, as described in Settimi, rather than to be sent to each individual source (e.g., health plan). Ex. 1003, ¶141. Specifically, a POSA would apply Settimi’s concept of a central warehouse to the embodiment in Fig. 4 of Evenhaim. <i>Id.</i> In that combination, each data source in Fig. 4 (PBM 1 through PBM n) would de-identify its patient records by creating an encrypted token, as described in Evenhaim, then send the patient records to a central warehouse. <i>Id.</i> Under this approach, the data warehouse would replace the PBMs shown in Evenhaim’s Fig. 4 as the data source. <i>Id.</i> Because the central warehouse contains only de-identified records, in which the PII has been replaced with an encrypted token, a POSA would have understood that the encrypted patient list sent in Evenhaim’s steps 3-4 would use encryption that allows for finding matching records in the central warehouse (e.g., creating a token for each individual in a group in the form of a unique encryption key). Ex. 1005, Fig. 4, 12:4-13:20; Ex. 1003, ¶142. Settimi also explains that the tokens are used to identify all the records for particular patients. Ex. 1006, [0035], [0037].

Claim Clause	Evenhaim in view of Settimi Ground
	 The flowchart, labeled FIG. 4, illustrates a process for request analysis and data aggregation. It begins with a 'Pharmaceutical Company Marketing Team' box at the top left. Below it, a sequence of steps is shown: 'Start every set frequency (monthly, quarterly, etc.)', followed by a red-bordered box containing '1. Request analysis of one or more Health Programs (such as program medication compliance rate vs. control)' and '* 2. Use Crossix user interface to define program components and upload identifiable patient lists'. This leads to a 'Final Analysis Result' box, which then points to an 'End' box. A central 'Crossix' box contains several steps: '* Data Aggregator encryption key', '* 3. Encrypt patient list and query' (also in a red-bordered box), '* 4. Distribute query to all available data sources', '* 6. Aggregate Analysis Results from each of the data sources to the Final Analysis Result', and '* 7. Deliver Final Analysis Result via Crossix User interface'. To the right, two 'Health Plan/PBM' boxes (labeled '1' and 'n') are shown. Each contains '* 5. Crossix data mining software perform name match and analysis' and 'Analysis Results'. These boxes also contain 'Identifiable patient-level micro-data'. Arrows indicate the flow of data and queries between the Crossix box and the Health Plan/PBM boxes, and from the Health Plan/PBM boxes back to the Crossix box. A legend at the bottom left states: '* Designates all Crossix related systems and responsibilities'. FIG. 4 In Evenhaim the tokens are produced for individuals in a group defined by a list provided in the request as shown in box 2. Ex. 1005, 8:18-22 (“[T]he instant method can ask about the status of Tom, Dick, Harry, and ... obtain results from that query.”), 6:64-67, 8:4-13, Fig. 4; Ex. 1003, ¶143. In Evenhaim’s box 4, the query, consisting of a list of encrypted tokens, would be sent to the data source (a central repository with de-identified patient records) that contains corresponding tokens that are matched to determine the relevant healthcare records responsive to the query. Ex. 1005, Fig. 4, 7; Ex. 1003, ¶144.

Claim Clause	Evenhaim in view of Settimi Ground
[7.c] wherein the identity of the individuals ... is unattainable from the tokens, each token being associated with a corresponding token in a set of de-identified healthcare data,	See 7.c (Ground 1) above. As discussed above, each produced token in the query is associated with a corresponding token in the de-identified healthcare information in the data warehouse. Ex. 1006, [0027], [0030], [0035] (“The de-identified patient data is then staged into a data warehouse 210 where it is available for querying.”), [0036], [0037] (“[C]reate[ing] patient cohort reports 212 based on the querying the longitudinal patient data is supported by the ability to connect all records relating to a single patient in the data warehouse 210. This requires a unique identifier to be associated with each patient record The unique identifier ... does not provide personal direct identifying information such as name, social security number, street address, etc.”), [0039]-[0041], [0042] (“The de-identified patient data includes an EPID 308 that may be useful in creating longitudinal reports that analyze more than one record for a particular patient.”); Ex. 1003, ¶146.
[7.d] and each token ... being associated with healthcare data for a corresponding individual;	See 7.d (Ground 1) above. Each corresponding token in the central warehouse is associated with healthcare data for a corresponding individual. Ex. 1006, [0027], [0030], [0035]-[0037], [0039]-[0042]; Ex. 1003, ¶148.
[7.e] a data server for producing the requested healthcare information that characterizes the group	See 7.e (Ground 1) above. For the reasons established above, Settimi’s central warehouse forms a data server for producing the requested healthcare information for the group of people listed in the query. Ex. 1006, [0035] (“[D]e-identified patient data is then staged into a data warehouse 210 where it is available for querying.”), [0037] (“[C]reate[ing] patient cohort reports 212 based on the querying the longitudinal patient data is supported by the ability to connect all records relating to a single patient in the data warehouse 210.”); Ex. 1003, ¶150.

Claim Clause	Evenhaim in view of Settimi Ground
[7.f] by identifying the tokens ... and ... de-identified healthcare data that correspond to the produced tokens,	Evenhaim shows this feature, as addressed above. See 7.f (Ground 1) above. In particular, Figs. 4 and 4A show how the produced tokens (“encrypt patient list”) from the aggregator are sent to the data server (see boxes 3-5). <i>Id.</i>, 152. In view of Settimi, the data server would be the centralized warehouse of de-identified patient records. <i>Id.</i> The centralized warehouse contains de-identified records from the various originating sources (e.g., Health Plan/PBMs 1-n in Fig. 4 of Evenhaim). In both Evenhaim and Settimi, the de-identification of healthcare records occurs by substituting an encrypted token into the record in place of the identifying data (e.g., a name). Ex. 1006, Figs. 1 and 2, [0027], [0037]-[0043]; Ex. 1003, ¶153. Settimi and Evenhaim describe similar schemes for creating encrypted tokens from PII. Ex. 1005, 12:4-13:20; Ex. 1003, ¶153. At the data server, in Evenhaim’s Fig. 4, box 5, the data source matches the query information against the de-identified patient records, matching the produced tokens to corresponding tokens in a set of de-identified patient records. Ex. 1005, 12:4-47. Moreover, because the central warehouse contains only de-identified data, 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. Ex. 1003, ¶153. Specifically, no names or other PII could be used in the query because the centralized warehouse has no such information. <i>Id.</i> Thus, a POSA would have understood, with the combination, that searching for particular patients, as described in Evenhaim, would be accomplished using the encrypted tokens inasmuch as that is the way the records are identified in Settimi’s centralized warehouse. Indeed, Settimi describes this type of search. <i>Id.</i>; Ex. 1006, [0037] (“This requires a unique identifier to be associated with each patient record that is transmitted to the data warehouse 210. The unique

Claim Clause	Evenhaim in view of Settimi Ground
	identifier indicates an anonymous or abstract patient.”), (“[Q]uerying the longitudinal patient data is supported by the ability to connect all records relating to a single patient in the data warehouse 210.”). Thus, the tokens sent from the aggregator are matched against the tokens in the de-identified patient records in the data source in order to retrieve the de-identified patient records requested. Ex. 1005, 12:13-16, 12:42-45. A POSA would understand that the token creation and matching in Evenhaim, when combined with the data warehouse of Settimi, would apply to the embodiment in Fig. 4 and 4A such that the data source in box 6 (the data warehouse) would have de-identified records with encrypted tokens that are identified in response to a query to the data sources sent in box 4. Evenhaim explains that the token creation could be performed on the aggregator as well as on the data sources. <i>Id.</i>, 12:26-34; Ex. 1003, ¶154.
[7.g] wherein the ... tokens ... are similarly encrypted,	A POSA would understand that similar encryption would be used on both the encryption server where the query is created (Evenhaim Fig. 4, boxes 3 and 4) and on the data server where the query is received, so that the sent tokens are matched to similarly encrypted tokens in de-identified patient records (shown in box 5). Ex. 1003, ¶155. Indeed, this is what allows the identification of the requested records. Ex. 1006, [0037]; Ex. 1003, ¶156. As discussed, the centralized warehouse from Settimi only has de-identified healthcare information that has tokens in the records because those records were de-identified prior to being loaded into the warehouse. Ex. 1006., Figs. 1 and 2, [0027], [0037]-[0043]; Ex. 1003, ¶156. To match those records for the query, the tokens created from PII on the encryption server (aggregator) are similarly encrypted to the tokens used to de-identify the patients sent to the data warehouse. This is accomplished by using the same or similar public

Claim Clause	Evenhaim in view of Settimi Ground
	encryption key as shown in Fig. 4 above box 3. Ex. 1005, 12:4-13:20; Ex. 1006, [0047] (explaining that that a user may search by the EPID), [0041]; Ex. 1003, ¶156.
[7.h] and ... information is absent personally identifiable information	See 7.h (Ground 1) above; <i>see also</i> Ex. 1006, [0027], [0030], [0035]-[0037], [0039]-[0042]. Also, a POSA would appreciate that further encryption could be used in the produced records to further mask the identification of the patients. Ex. 1003, ¶42
[7.i] and has been produced without the individuals ... having authorized production ...; and	Both Evenhaim and Settimi describe that using tokenization in de-identified healthcare information complies with HIPAA, and is an alternative option to obtaining explicit patient authorizations from the individuals in the group. As discussed in Ground 1, Evenhaim describes producing healthcare information without authorization from individuals in the group in accordance with HIPAA. Ex. 1005, 3:17-31 (“Health transaction data is protected by privacy standards such as the HIPAA ... by properly de-identifying transaction data from patient identifiers”), 4:34-48, 5:46-6:10, 8:18-22, 14:7-13 (“In each ‘query relationship’ there are different legal standards which may be applicable—such as ... HIPAA ... de-identified without micro-data specific content or substantially equivalently provably statistically intractable.”), 15:15-24, 14:59-67; Ex. 1003, ¶¶158-60. Per HIPAA, the purpose of de-identification is to create shareable data that does not require permission from each patient whose information is shared. HIPAA, 45 C.F.R. § 164.502(d); Ex. 1001, 1:33-36, 4:1-3. Settimi also describes using a token system for the purpose of complying with HIPAA, as an alternative to obtaining patient authorization under HIPAA’s Privacy Rule. Ex. 1006, [0009] (“The removal of identifying information must be performed per the federal Health Insurance Portability

Claim Clause	Evenhaim in view of Settimi Ground
	and Accountability Act (HIPAA) regulations.”), [0014], [0017], [0027] (“The terms ‘de-identified patient information’ and ‘de-identified patient data’ ... refer to both fully de-identified data as defined by HIPAA and limited data set data as defined by HIPAA.”), [0039]-[0040]; Ex. 1003, ¶161.
[7.j] providing the produced healthcare information ...	See 7.b (Ground 1) above; <i>see also</i> Ex. 1006, [0027], [0030], [0035]-[0037], [0039]-[0042]; Ex. 1003, ¶162.
[7.k] absent authorization ... from the individuals	See 7.i above; <i>see also</i> Ex. 1006, [0027], [0039]-[0040]; Ex. 1003, ¶163.
[8] The system of claim 7, wherein the healthcare information ... is in conformity with ... (HIPAA).	See 7.i (Ground 1) above.
9. The system of claim 7, wherein the request ... includes personally identifiable information associated with members	See 9 (Ground 1) above.
10. The system of claim 7, in which producing the requested healthcare information includes encrypting	See 10 (Ground 1) above.
11. The system of claim 7, in which producing the requested healthcare	See 11 (Ground 1) above.

Claim Clause	Evenhaim in view of Settimi Ground
information includes identifying ... a minimum number	
12. The system of claim 7, in which producing the requested healthcare information includes determining ... a minimum number of individuals.	See 11 above.
13. The system of claim 7, in which the healthcare data represents medical related information	See 13 (Ground 1) above.

Claim Clause	Evenhaim in view of Settimi Ground
[1.a] A computer-implemented method comprising: receiving a request for healthcare information that characterizes a group ..., the healthcare information being assembled from healthcare data that comprises de-identified information;	See 7.a, 7.b, 9 above.
[1.b] producing, by a processor of an	See 7.a, 7.b above.

Claim Clause	Evenhaim in view of Settimi Ground
encryption server, tokens,	
[1.c] wherein the identity of the individuals ... is unattainable from the tokens, each token being associated with an individual ..., each token being associated with a corresponding token in a set of de-identified healthcare data, and	See 7.c above.
[1.d] each token ... being associated with healthcare data for a corresponding individual;	See 7.d above.
[1.e] when the group includes at least a minimum number of individuals,	See 11 above.
[1.f] producing the requested healthcare information that characterizes the group by identifying the tokens ... and ... de-identified healthcare data ...,	See 7.f, 7.h above.
[1.g] wherein the ... tokens ... are similarly encrypted, and	See 7.g, 7.i above.

Claim Clause	Evenhaim in view of Settimi Ground
[1.h] ... information is absent personally identifiable information and	See 7.j above.
[1.i] has been produced without the individuals ... having authorized production ...; and	See 7.k above.
[1.j] providing the produced healthcare information	See 7.b, 7.j, 7.k above.
[2] The computer-implemented method of claim 1, wherein the healthcare information ... is in conformity with ... (HIPAA).	See 8 above.
[3] The computer-implemented method of claim 1,... receiving personally identifiable information associated with members of the group	See 9 above.
[4] The computer-implemented method of claim 1, in which producing the requested healthcare information includes encrypting	See 10 above.
[5] The computer-implemented method of claim 1, in which	See 11 above.

Claim Clause	Evenhaim in view of Settimi Ground
producing the requested healthcare information includes identifying at least a minimum number	
[6] The computer- implemented method of claim 1, in which the healthcare data represents medical related information	See 13 above.
[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:	See 7.a above.
[14.b] receiving a request for healthcare information that characterizes a group ..., the healthcare information being assembled from ... de-identified information;	See 7.b above.
[14.c] producing, by a processor of an	See 7.a, 7.b, 7.f above.

Claim Clause	Evenhaim in view of Settimi Ground
encryption server, tokens,	
[14.d] wherein the identity of the individuals in the group is unattainable ...;	See 7.c, 7.d above.
[14.e] when the group includes ... a minimum number of individuals,	See 11 above.
[14.f] producing the requested healthcare information ... by identifying the tokens ...,	See 7.f above.
[14.g] wherein the ... tokens ... are similarly encrypted, and	See 7.g above.
[14.h] the produced healthcare information is absent personally identifiable information ...; and	See 7.i above.
[14.i] providing the produced healthcare information to report the characteristics of the group ... absent authorization	See 7.j above.
[15] The computer readable storage devices of claim 14, wherein the healthcare information provided	See 7.i above.

Claim Clause	Evenhaim in view of Settimi Ground
... is in conformity with ... (HIPAA).	
[16] The computer readable storage devices of claim 14, wherein the request for healthcare information ... includes personally identifiable information	See 9 above.
[17] The computer readable storage devices of claim 14, in which producing the requested healthcare information includes encrypting	See 10 above.
[18] The computer readable storage devices of claim 14, ... identifying at least a minimum number of corresponding tokens.	See 11 above.
[19] The computer readable storage devices of claim 14, in which the healthcare data represents medical related information	See 13 above.

E. DICK GROUNDS

i. Ground 3: Obvious over Dick in view of Landi

Dick in view of Landi establishes that claims 7-10 and 13 are unpatentable. Ex. 1003, ¶199.

Dick, a U.S. patent application published on August 15, 2002, qualifies as prior art under at least 35 U.S.C. § 102(b) (pre-AIA).

Dick describes a system for requesting and retrieving de-identified medical information for a group of individuals where a first server sends a query that characterizes the group to a second server (medical repository) that returns de-identified healthcare information in response to the query. Ex. 1007, Abstract, [0024], claim 23; Ex. 1003, ¶¶54, 200. Dick explains that its system can be used to obtain healthcare information for many purposes, including for health insurance risk assessment of the individuals for policy underwriting. Ex. 1007, [0003], [0026], [0037], [0041]-[0042], [0047]; Ex. 1003, ¶¶54, 200.

For instance, Dick's Fig. 2 shows "a request for medical information" that "include[es] identification of a subject." Ex. 1007, Fig. 2. Dick explains that the "subject" may be "a group of humans" and that the requester may be a medical "insurance agenc[y]." *Id.*, [0024]-[0025], claims 23-24. That request is transmitted "to a medical information repository," which returns de-identified medical records in response to the request. Ex. 1007, Fig. 2; Ex. 1003, ¶¶54-55.

Dick describes that, under HIPAA, either explicit consent for transmitting the healthcare information must be obtained from the patients or the information can be sent without authorization if de-identified. Ex. 1007, [0044]-[0045]. De-identification can take place at the medical repository or originating source of the information, and a POSA would understand it could use “de-identifying methods and processes” but Dick does not describe any specific de-identification methods. Ex. 1007, [0013], [0046]; Ex. 1003, ¶201. Therefore, a POSA relying on Dick would naturally look elsewhere in order to implement the de-identification called for in Dick. Ex. 1003, ¶201.

Landi sets forth a de-identification method as called for in Dick. Specifically, Landi describes a token matching system used to de-identify medical records, such as the records referred to in Dick. Ex. 1003, ¶¶58, 202.

Landi describes how different healthcare organizations de-identify their records by creating an encrypted token (an encrypted form of the PII such as a name or SSN). Ex. 1008, 2:30-53, 5:13-19; Ex. 1003, ¶58-60. Each “Encrypted ID,” as Landi terms them, is “sufficient to uniquely identify the patient” and may be stored with the corresponding medical record(s). Ex. 1008, 5:13-36. The de-identified patient records may be released to third-party entities without compromising patient privacy. Ex. 1008, 5:41-44. The de-identified medical records are stored in a central data server that can be queried, much like Dick’s

medical repository. Ex. 1008, 4:11-28, 7:3-38, 8:16-19, 8:61-63, 10:15-54, 11:52-63 (“can readily be searched”).

Like Dick, Landi’s purpose is compliance with HIPAA. Ex. 1008, 1:58-2:18, 3:52-57, 9:20-29, 10:3-31, 11:64-12:67. And, both references are directed to using central repositories to provide a collection of medical records for searching. Ex. 1007, Fig. 2, [0003], [0008], [0011], [0024]; Ex. 1008, 4:40-46, 11:23-29. Thus, a POSA would have been motivated to use Landi’s de-identification system in which PII is encrypted to form an Encryption ID and the de-identified records are stored in a central database for querying. Ex. 1003, ¶203. In particular, Landi explains that prior methods simply stripped PII and that its method improved on such systems through the use of Encryption IDs created using a common public key that allowed for the same patient to be recognized “even though the identity of the person remains unknown.” Ex. 1008, 2:19-26, 8:38-35, 8:47-55, 11:3-29, 9:43-60; Ex. 1003, ¶60-61. Moreover, Landi explains that, under HIPAA, (i) all de-identification must occur at the clinical site, which is why the central data server (*i.e.*, system 30) contains only de-identified medical records and (ii) the public key for creating the Encryption ID is shared with all parties (and not a violation of HIPAA). Ex. 1008, 10:52-63, 8:38-55, 7:3-10.

Thus, a POSA would readily appreciate that, when using Landi’s central database of de-identified medical records, which contain associated Encryption IDs

created with freely distributable public keys, in Dick’s system for searching a central database (Ex. 1007, [0011], [0025]) for a “group” of individuals (Ex. 1006, [0024]), one would use the public key to create the list of Encrypted IDs to be used in the query to the central database. Ex. 1003, ¶204. Indeed, the very purpose of Landi’s Encrypted IDs is so that each “patient can be recognized” without exposing the identity of any person. Ex. 1008, 8:38-55; Ex. 1003, ¶204. Further, because the central database includes only the de-identified records, a POSA would understand that searching for a group using anything other than their Encrypted IDs would not return proper results. Ex. 1003, ¶205. Thus, to use Landi’s system properly, a POSA would have found it obvious to use the freely distributable public key in Dick’s query to the central database (*e.g.*, step 105 in Fig. 2). *Id.* In fact, Dick explains that its query would use any “identification characteristics capable of being correlated with stored medical information.” Ex. 1007, [0024].

Landi describes to a POSA how to encrypt private patient data using tokens (for example by hashing), which can be used to match a patient’s de-identified records, and which cannot be reversed engineered. Ex. 1003, ¶¶61-64. Given each reference employs a central database of medical records for searching and Landi simply uses known encryption techniques, a POSA would have had a reasonable expectation of success combining Dick and Landi, particularly given their similar

environments. Indeed, as discussed above, tokenization to protect sensitive information was well known in the field. Ex. 1003, ¶206. Moreover, Dick calls for the very de-identification described in Landi.

The claim chart below shows that the claims 7-10 and 13 are obvious over Dick in view of Landi. Ex. 1003, ¶99.

Claim Clause	Dick in view of Landi Ground
[7.a] A system comprising: an encryption server, having a processor and a memory,	Dick describes a “Requester’s Server” (230) that receives the names of a group of individuals from a “Requesting & Viewing Client,” and then creates a query that it transmits, in connection with central server 245, to a “Medical Information Repository.” Ex. 1007, Fig. 3, [0022], [0028], [0034], claim 23. The query is for de-identified healthcare information in order to comply with HIPAA. Ex. 1006, [0044]-[0046]. Dick’s requester’s server (and associated central server) is on a network and includes standard computer elements. <i>Id.</i>, [0020] (“internet-based”), [0036], [0048] (“general purpose computer”, “appropriate hardware”, “memory”), [0049]. A POSA would have found it obvious that Dick’s Requester’s Server has a processor and a memory. Ex. 1003, ¶¶207-09. Landi describes using encryption to create tokens from PII using a public encryption key. Ex. 1008, 2:63-67, 3:3-5, 8:38-55 (“public keys are freely distributable”), 14:29-32. Landi also establishes that these computerized systems use “processors” and “program storage devices.” Ex. 1008, 3:58-4:10; Ex. 1003, ¶¶208-09.
[7.b] for producing a token for each individual included in a group ... identified in a request for healthcare	Dick’s Requester’s Server (encryption server) receives a request for medical records for a “subject” that may be “a human individual or group of humans.” Ex. 1007, Figs. 1-3, [0024], [0044]-[0046], claim 23 (“a group of preselected individuals”), Abstract (“The present

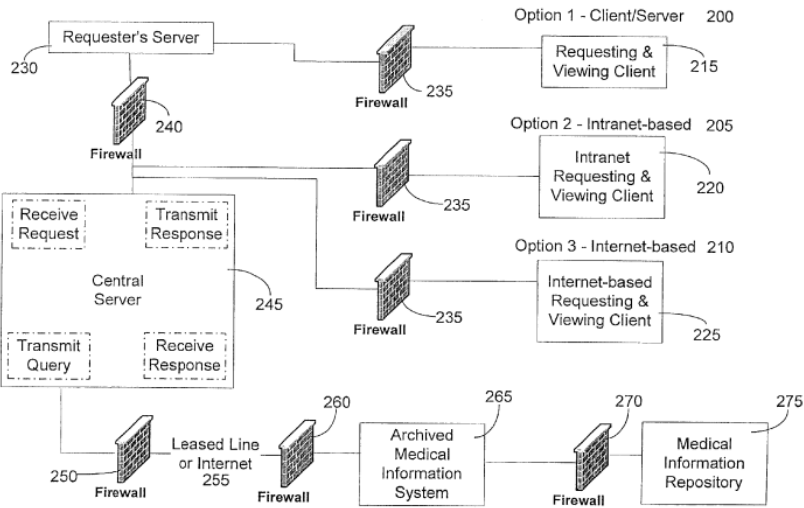
Claim Clause	Dick in view of Landi Ground
information that characterizes the group,	invention relates to a method of searching for medical information ... compris[ing] the steps of receiving a request for medical information including identification of a subject; transmitting a query to a medical information repository for information pursuant to the request.”); Ex. 1003, ¶210. The request for medical records is to be sent to a repository containing associated medical records. Ex. 1007, [0011], [0019]; Ex. 1003, ¶210. Dick describes that its system can be used to obtain healthcare information for many purposes, including in connection health insurance risk assessment of the individuals for policy underwriting. Ex. 1007, [0003], [0026], [0037], [0041]-[0042], [0047]; Ex. 1003, ¶210. As described above and below, Landi’s central database/system 30 containing medical records for searching includes solely de-identified records in which PII has been replaced with a token in the form of Encrypted IDs for each individual that has patient records. Ex. 1008, 4:40-46 (“[T]he public keys ... are used for de-identifying (encrypting) one or more items of patient identifying information ... to generate an encrypted version of the patient identifying information (referred to herein as ‘Encrypted IDs’.”), 11:23-29 (“[E]ach Encrypted ID is a unique reproducible encrypted version of patient identifying information, the process preserves patient uniqueness to enable to the same patient to be recognized.”); Ex. 1003, ¶211-12. The Encrypted IDs are created using public keys that are freely distributable so that various entities may replicate the Encrypted IDs when dealing with the same patient. Ex. 1008, 8:39-55, 4:65-5:19, 5:32-44, 5:57-61; Ex. 1003, ¶211. Thus, as also discuss above, a POSA would have been motivated to produce a token for each individual in Dick’s group of individuals in a query because (i) the

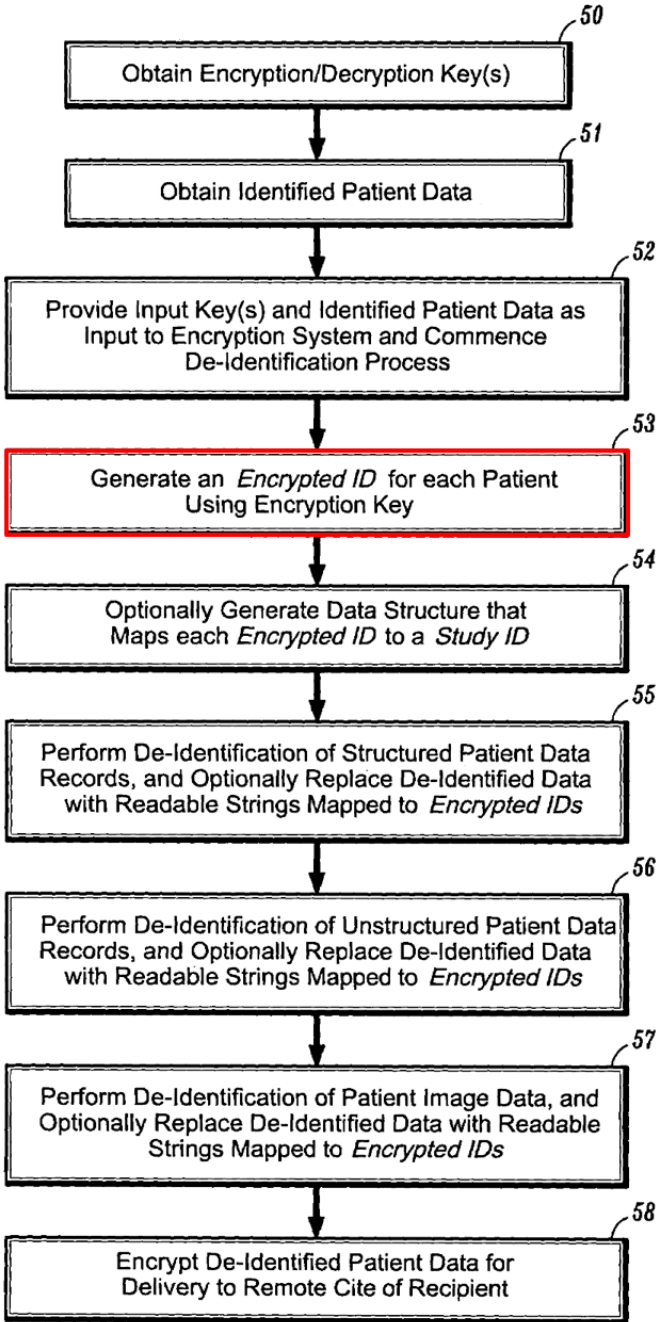
Claim Clause	Dick in view of Landi Ground
	purpose of Dick’s system is to query a remote database for medical records for the group of individuals (Ex. 1007, Fig. 2, [0003], [0008], [0011], [0024]), (ii) Landi’s central database of de-identified patient records identifies the records through Encrypted IDs (tokens) (Ex. 1008, 7:3-38), and (iii) the public keys for creating such tokens are freely distributed in compliance with HIPAA in order to allow for recognition of corresponding records (Ex. 1008, 8:39-55). Ex. 1003, ¶¶213, 215. Specifically, the tokens created with the public key would allow for identification of corresponding medical record in the de-identified, central database. See Ex. 1007, claim 23, (“A method for gathering and formatting medical information regarding an individual,... comprising the steps of: (a) searching at least one medical information repository for medical information regarding a group of preselected individuals.”). Thus, a POSA applying the token creation and matching system in Landi to Dick would understand that the Requester’s Server (encryption server) in Dick would query de-identified patient records held on a data server (Medical Information Repository in Dick and/or central repository in Landi) using the public encryption key from Landi to create encrypted tokens to be used for such requests. Ex. 1008, 8:49-52(“[T]he public keys can be used to produce a unique, reproducible encrypted version of patient identifying information. Since the encryption is reproducible, the same patient can be recognized”); Ex. 1003, ¶213. A POSA would have understood that creating encrypted tokens on the Requester’s Server using Landi’s method complies with HIPAA. Ex. 1008, 1:58-2:26, 3:52-57, 9:20-27, 10:23-31, 11:64-12:67; Ex. 1007, [0004], [0024], [0026]; Ex. 1003, ¶214. For example, it would potentially violate HIPAA to just send PII to be used for such a query directly to the centralized data server (45 C.F.R. § 164.502(d)), so in order to avoid a potential HIPAA violation it was common practice to use a public

Claim Clause	Dick in view of Landi Ground
	encryption key to create tokens on a requesting server when sending a query. Ex. 1003, ¶214.
[7.c] wherein the identity of the individuals ... is unattainable from the tokens, each token being associated with a corresponding token in a set of de-identified healthcare data,	The purpose of the tokens (Encrypted IDs) from Landi is to prevent identification of the individuals. Ex. 1008, 7:22-30, 11:13-17 (“The Encrypted ID for each patient is generated such that the patient identifying information contained within the Encrypted ID cannot be reconstructed without a valid decryption key (e.g., private key).”). Specifically, Landi explains that the public key allows for encryption of the PII, but does not allow for decryption—only the private key (which is not disseminated) allows for decryption. <i>Id.</i>, 4:35-48, 5:2-31, 7:34-38, 11:13-19; Ex. 1003, ¶216. As discussed above, each token created for purposes of the query is associated with a corresponding token in the de-identified health records in a central database, such as Landi’s central system 30. Indeed, the very purpose of disseminating a public key to create tokens is to allow for identification of corresponding patient records. Ex. 1008, 8:38-55; Ex. 1003, ¶216. Specifically, per Landi, the medical records from the various sources are de-identified, before being sent to the central repository, by encrypting the PII of the individual to create a token and removing the PII. Ex. 1008, 4:11-28, 5:32-44 (“generate Encrypted IDs and then store each Encrypted ID with or within a corresponding de-identified data patient data record (i.e., a patient data records from which patient identifying information has been removed”); 7:3-10 (“The central patient data processing system (30) comprises a repository of persistently stored de-identified patient data records (35) containing de-identified (encrypted) patient identifying information, which are collected from different clinical sites.”), 9:43-60; 5:41-47 (“The encrypted (de-identified) patient data (Encrypted IDs) can be included in de-

Claim Clause	Dick in view of Landi Ground
	identified patient records, which can be released to third-party entities without compromising patient privacy.”), 8:47-55, 11:23-29 (“[E]ach Encrypted ID is a unique reproducible encrypted version of patient identifying information, the process preserves patient uniqueness to enable to the same patient to be recognized at different collection times. In other words, this process ensures that if data is collected more than once from a particular patient, the patient will be mapped to the same Encrypted ID.”); Ex. 1003, ¶217. Thus, because the public keys created matching tokens (in the query and in the de-identified records), the tokens (Encrypted IDs) stored in Landi’s central processing system 30 correspond to tokens in the query. Ex. 1008, 4:11-34, 7:3-38, 8:38-9:10, 9:43-10:14 (“(1) to comply with HIPAA, analysis must be done on de-identified data when the persons analyzing patient data are not associated with the provider organization; (2) data is collected at various points of time and analyses are performed after each data collection.”), Figs. 1-3. Landi also describes where tokens would be matched when querying for patient records associated with a clinical trial where “each time data is collected, the patient should be de-identified in the same way” in order to create a first token to be used to query the patient records. Ex. 1008, 9:43-60. Landi also describes other situations where the de-identified patient database is queried. <i>Id.</i>, 7:3-10, 8:47-55, 10:52-63, 11:23-29, claim 15 (“[U]sing the encrypted ID ... to recognize a subject patient of patient data records collected at different times.”). Therefore, a POSA implementing Landi’s token matching system on Dick would understand that each token created for the query on the Requester’s Server would match a corresponding token in Medical Information Repository’s de-identified patient records. In that way the relevant de-identified healthcare

Claim Clause	Dick in view of Landi Ground
	information related to patients in a clinical trial (or a query from a health insurance company) could be retrieved for analysis while complying with HIPAA. Ex. 1003, ¶218
[7.d] and each token ... being associated with healthcare data for a corresponding individual;	As established above, Landi describes that the healthcare data stored in the central system/database 30 (and thus in Dicks' repository) is de-identified by encrypting the PII into a token, and that token is associated with patient records. Ex. 1008, 3:1-5 (“[T]he encrypted ID comprises an encrypted representation of one or more items of individual identifying information, and wherein the encryption system can generate de-identified data records of the individual which are associated with the encrypted ID.”); Ex. 1003, ¶¶219-20. Specifically, in Landi's central system/database 30, each Encrypted ID (token) is (i) an encrypted version of an individual's PII and (ii) stored “with or within a corresponding de-identified [] patient data record.” Ex. 1008, 5:32-36, 8:38-55, 7:3-21, 2:60-3:13, 4:35-48, 5:2-31; Ex. 1003, ¶¶219-20.
[7.e] a data server for producing the requested healthcare information that characterizes the group	As established above, Dick describes a data server for producing the healthcare information that characterizes the group in the form of a medical information repository. Ex. 1007, Fig. 3, [0019], [0028] (“Following receipt of the request for information 105, the Central Server 245 will transmit a query to a medical information repository 275 for information pursuant to the request 115. ... The most common forms of communication are depicted in FIG. 2 as leased line or internet 255. In addition, as shown in Fig. 3, an Archive Medical Information System (AMIS) server 265 may be accessed by the central server 245. AMIS server 265 will receive the transmitted query 115 and proceed to search the AMIS database for information in satisfaction of the query.”); Ex. 1003, ¶221.

Claim Clause	Dick in view of Landi Ground
	 FIG. 3 Dick explains that the repository responds to queries. Ex. 1007, claim 23 (“(b) compiling and formatting at the site of the medical information repository the results of the search in a generic format ascertainable by requester;... (d) providing the compiled and de-identified results of at least one of the preselected individuals to a requester”). Moreover, Landi’s central database/system 30 is a data server in that it is a networked computer system that stores de-identified medical records for the purpose of sharing in response to third-party queries. Ex. 1008, 7:3-31, 8:16-55, 10:52-65. A POSA would have readily understood that Landi’s manner of storing de-identification data could be used with or in place of Dick’s repository. Ex. 1003, ¶221
[7.f] by identifying the tokens ... and ... de-identified healthcare data that correspond to the produced tokens,	The tokens in queries sent from the Requester’s Server (encryption server) in Dick would correspond to the similarly encrypted tokens in the de-identified patient records in the medical information repository or central system 30 (data server), per Landi’s teachings discussed

Claim Clause	Dick in view of Landi Ground
	above. Landi describes tokens in a set of de-identified healthcare data and the associated healthcare data that would correspond to the produced tokens. Ex. 1008, Fig. 3; Ex. 1003, ¶222.  <pre> graph TD 50[Obtain Encryption/Decryption Key(s)] --> 51[Obtain Identified Patient Data] 51 --> 52[Provide Input Key(s) and Identified Patient Data as Input to Encryption System and Commence De-Identification Process] 52 --> 53[Generate an Encrypted ID for each Patient Using Encryption Key] 53 --> 54[Optionally Generate Data Structure that Maps each Encrypted ID to a Study ID] 54 --> 55[Perform De-Identification of Structured Patient Data Records, and Optionally Replace De-Identified Data with Readable Strings Mapped to Encrypted IDs] 55 --> 56[Perform De-Identification of Unstructured Patient Data Records, and Optionally Replace De-Identified Data with Readable Strings Mapped to Encrypted IDs] 56 --> 57[Perform De-Identification of Patient Image Data, and Optionally Replace De-Identified Data with Readable Strings Mapped to Encrypted IDs] 57 --> 58[Encrypt De-Identified Patient Data for Delivery to Remote Cite of Recipient] </pre> FIG. 3

Claim Clause	Dick in view of Landi Ground
	In particular, Landi explains that the tokens in the de-identified records in the central system/database 30 are used to recognize (<i>i.e.</i>, identify) the records that match the corresponding tokens created by encrypting the same patient information elsewhere using the common public key. Ex. 1008, 8:38-55, 11:23-29 (“enable [] the same patient to be recognized”), 11:52-63 (“can readily be searched”).; Ex. 1003, ¶222 And, Dick’s search request involves a search for patient records for a specified group of patients, as discussed above.
[7.g] wherein the ... tokens ... are similarly encrypted,	Landi describes that various entities create tokens (Encrypted IDs) using the same public keys that are freely shared. Ex. 1008, 8:47-55, 11:3-29, 4:65-5:2 (“same secure public encryption protocol (e.g., RSA)”), 4:35-40, 5:7-5:36 (“master public key”; “public key”; “to thereby generate an Encrypted ID for each subject patient”), 10:40-51; Ex. 1003, ¶223. Additionally, a POSA implementing the token matching system in Landi into Dick’s query would be motivated to use the same or similar public encryption key to enable the desired healthcare information to be properly searched for matching records. Ex. 1007, claim 23; Ex. 1003, ¶223.
[7.h] and ... information is absent personally identifiable information	Landi explains that the produced healthcare information is absent PII because the healthcare information can be produced to third parties without compromising the patient privacy. Ex. 1008, 5:32-47 (“stored de-identified patient data records (25-1~25-n) ... having corresponding Encrypted IDs ... which can be released to third-party entities without compromising patient privacy.”), 2:30-54, 13:41-53, 2:5-26; Ex. 1003, ¶¶224-25.

Claim Clause	Dick in view of Landi Ground
[7.i] and has been produced without the individuals ... having authorized production ...; and	Dick describes producing healthcare information without the individuals in the group having authorized production. Ex. 1007, [0024], [0026] (“In some cases, consent of the subject(s) is required to obtain the medical information.... In other instances, where the law does not require a release, none is obtained.”), [0047]; Ex. 1003, ¶226. Landi also produces healthcare information without the individuals in the group having authorized production in that the very purpose of Landi’s system is to comply with the HIPAA requirements for such disclosure. Ex. 1008, 1:5-18 (“The HIPAA Privacy Rule allows for certain entities to ‘de-identify’ protected health information for certain purposes so that such information may be used and disclosed freely, without being subject to the protections afforded by the Privacy Rule.... The Privacy Rule requirements do not apply to information that has been de-identified.”) Ex. 1003, ¶226. A POSA would have appreciated that the purpose of de-identification in Dick and Landi is to be able to disclose healthcare records without patient authorization. Ex. 1003, ¶227.
[7.j] providing the produced healthcare information to report the characteristics² of the group ...	See 7.b above. Further, Dick explains that the healthcare information is of the type used by insurance companies for underwriting purposes. Ex. 1007, [0003], [0012] (“claims handling, medication information”), [0025], [0035], [0038] (“tests ordered, results obtained”); <i>see also</i> Ex. 1008, 2:54-59, 6:4-18.

² The ’641 patent indicates that the characteristics of the group relate to “characteristics of the individuals” in the group that may be used to, for instance, score the group for underwriting purposes. Ex. 1001, 2:1-9, 4:41-54. Such information may relate to medical claims and prescription information. *Id.*, 6:6-8.

Claim Clause	Dick in view of Landi Ground
[7.k] absent authorization ... from the individuals	See 7.i above.
[8] The system of claim 7, wherein the healthcare information ... is in conformity with ... (HIPAA).	See 7.b above.
9. The system of claim 7, wherein the request ... includes personally identifiable information associated with members	Dick explains that the request for healthcare information identifies individuals in a group for which the data is sought. Ex. 1007, Fig. 1, box 105 (“Receiving a request for medical information, the request including identification of a subject.”), [0024] (“[S]ubject[s] might consist of a human individual or group of humans.”), [0019]-[0022], claim 23 (“[S]earching at least one medical information repository for medical information regarding a group of preselected individuals.”); Ex. 1003, ¶231. In Landi the request for healthcare information includes PII associated with members of the group because the Encrypted ID that are used in the query are created from PII associated with the patients. Ex. 1008, 4:40-47 (“[T]he public keys ... are used for de-identifying (encrypting) one or more items of patient identifying information ... to generate an encrypted version of the patient identifying information (referred to herein as ‘Encrypted IDs’.”); Ex. 1003, ¶232. For example, Landi describes how its invention can be used to monitor patients in a clinical trial for compliance while still complying with HIPAA. Ex. 1008, 9:43-10:15; Ex. 1003, ¶232. A POSA would have appreciated that when patients are queried under this scenario, the tokens are created using the PII for each patient in the trial (i.e. the group in question). Ex. 1008, 9:52-56 (“[E]ach time data is collected, the patient should be de-identified in the same way (e.g., it is critical to know that de-identified patient 24 from a first round of collection is also present

Claim Clause	Dick in view of Landi Ground
	in a second round and is still de-identified as de-identified patient 24).”); Ex. 1003, ¶232.
10. The system of claim 7, in which producing the requested healthcare information includes encrypting	As discussed above for claim 7, Landi describes producing the requested healthcare information includes encrypting respective data that identifies each individual to create the Encrypted IDs (tokens). Ex. 1008, 2:41-49 (“[G]enerating an encrypted ID for the individual, wherein the encrypted ID comprises an encrypted representation of one or more items of individual identifying information.”), 14:26-29, 4:40-47; Ex. 1003, ¶233.
13. The system of claim 7, in which the healthcare data represents medical related information	As explained above, Dick describes that the query from the Requester’s Server is for healthcare information that characterizes the group of individuals in the query. Ex. 1007, Abstract (“[A] method of searching for medical information ... compris[ing] the steps of receiving a request for medical information including identification of a subject; transmitting a query to a medical information repository for information pursuant to the request;”), [0024] (explaining that the searched for “subject might consist of a human individual or group of humans. The subject is the target of the search for medical information”), [0003], [0026], [0037], [0041]-[0042], [0047]; Ex. 1003, ¶234. In Landi the healthcare data represents medical related information associated with the individuals of the group, such as those in a clinical trial. Ex. 1008, 8:61-9:19 (“Systems and methods according to the invention for deidentifying patient data can be implemented for various purposes such as research, public health or healthcare operations.”), 9:43-60, 4:19-23; Ex. 1003, ¶¶27, 234.

i. Ground 4: Obvious over Dick in view of Landi and Murphy

Dick in view of Landi and Murphy establish that claims 1-6, 11, 12, and 14-19 are unpatentable. Ex. 1003, ¶235.

Murphy is an article titled “A Security Architecture for Query Tools used to Access Large Biomedical Databases,” which published in November 2002. Ex. 1009; Ex. 1013, ¶¶38-45. Murphy is prior art under at least 35 U.S.C. § 102(b) (pre-AIA). See Ex. 1013, ¶¶38-45.

Murphy describes techniques to prevent the identification of individuals in a search on a medical database. Ex. 1009, 552-53; Ex. 1003, ¶66. Murphy did this by ensuring that more than one individual is returned from a search. Ex. 1009, 555; Ex. 1003, ¶66. Murphy discloses an algorithm which blocks queries that return fewer than 3 patients thereby protecting patient identity. Ex. 1009, 555; Ex. 1003, ¶66. Allowing a search for one patient, even if de-identifying the results, would not mask the identity of the patient. Ex. 1003, ¶66.

A POSA would combine Dick and Landi with Murphy because Murphy describes how to use query responses that maintain patient privacy (a goal of Dick and Landi) using volume to mask patient identity, which complies with HIPAA. *Id.*, ¶236. Specifically, Murphy recommends at least a minimum amount of de-identified medical data (i.e., multiple patient records) such that the query complies

with the HIPAA statistical requirements. *Id.*, ¶237. This prevents a search for a single subject in Dick resulting in identification of the subject’s medical records.

A POSA would find the combination obvious because Landi is intended to comply with HIPAA. Ex. 1008, 2:5-18; 45 C.F.R. § 164.514(b); Ex. 1003, ¶236. Similarly, Dick cites to complying with the applicable privacy laws using statistically sound methods. Ex. 1007, [0046] (“[T]he medical information repository may instead release medical information upon condition that a person with appropriate knowledge and experience with generally accepted statistical and scientific principles has applied a ‘de-identifying’ methodology to remove or make certain that no personally identifiable information is released from the repository.”); Ex. 1003, ¶236.

A POSA would have had a reasonable expectation of success in making this combination inasmuch as preventing the return of a query with fewer than three patient records would have been a simple programming task in systems already designed to return search results. Ex. 1003, ¶238.

The application of Dick in view of Landi and Murphy to representative claims 11 and 12 is detailed below.

Claim Clause	Dick in view of Landi and Murphy Ground
11. The system of claim 7, in which producing the requested healthcare information includes	See claim 7 above. While Dick describes using statistical methods to ensure that an individual’s medical records are not identified, it

Claim Clause	Dick in view of Landi and Murphy Ground
identifying ... a minimum number	does not explicitly identify one well-known method of accomplishing that goal—preventing the return of, e.g., one record that can be associated a particular patient in view of the search parameters. Ex. 1007, [0046]; Ex. 1003, ¶241. 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.
12. The system of claim 7, in which producing the requested healthcare information includes determining ... a minimum number of individuals.	See claim 11 above.

Claim Clause	Dick in view of Landi and Murphy Ground
[1.a] A computer-implemented method comprising: receiving a request for healthcare information that characterizes a group ..., the healthcare information being assembled from healthcare data that	See 7.a, 7.b, 9 (Ground 3) above.

Claim Clause	Dick in view of Landi and Murphy Ground
comprises de-identified information;	
[1.b] producing, by a processor of an encryption server, tokens,	See 7.a, 7.b (Ground 3) above.
[1.c] wherein the identity of the individuals ... is unattainable from the tokens, each token being associated with an individual ..., each token being associated with a corresponding token in a set of de-identified healthcare data, and	See 7.c (Ground 3) above.
[1.d] each token ... being associated with healthcare data for a corresponding individual;	See 7.d (Ground 3) above.
[1.e] when the group includes ... a minimum number of individuals,	See 11 (Ground 3) above.
[1.f] producing the requested healthcare information that characterizes the group by identifying the tokens ... and the associated de-identified healthcare data ...,	See 7.f, 7.h (Ground 3) above.
[1.g] wherein the ... tokens ... are similarly encrypted, and	See 7.g, 7.i (Ground 3) above.

Claim Clause	Dick in view of Landi and Murphy Ground
[1.h] ... information is absent personally identifiable information and	See 7.j (Ground 3) above.
[1.i] has been produced without the individuals ... having authorized production ...; and	See 7.k (Ground 3) above.
[1.j] providing the produced healthcare information	See 7.b, 7.j, 7.k (Ground 3) above.
[2] The computer-implemented method of claim 1, wherein the healthcare information ... is in conformity with ... (HIPAA).	See 8 (Ground 3) above.
[3] The computer-implemented method of claim 1,... receiving personally identifiable information associated with members of the group	See 9 (Ground 3) above.
[4] The computer-implemented method of claim 1, in which producing the requested healthcare information includes encrypting	See 10 (Ground 3) above.
[5] The computer-implemented method of claim 1, in which producing the requested healthcare information includes identifying at least a minimum number	See 11 (Ground 3) above.

Claim Clause	Dick in view of Landi and Murphy Ground
[6] The computer-implemented method of claim 1, in which the healthcare data represents medical related information	See 13 (Ground 3) above.
[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:	See 7.a (Ground 3) above.
[14.b] receiving a request for healthcare information that characterizes a group ..., the healthcare information being assembled from ... de-identified information;	See 7.b (Ground 3) above.
[14.c] producing, by a processor of an encryption server, tokens,	See 7.a, 7.b, 7.f (Ground 3) above.
[14.d] wherein the identity of the individuals in the group is unattainable ...;	See 7.c, 7.d (Ground 3) above.
[14.e] when the group includes ... a minimum number of individuals,	See 11 (Ground 3) above.
[14.f] producing the requested healthcare	See 7.f (Ground 3) above.

Claim Clause	Dick in view of Landi and Murphy Ground
information ... by identifying the tokens	
[14.g] wherein the ... tokens ... are similarly encrypted, and	See 7.g (Ground 3) above.
[14.h] the produced healthcare information is absent personally identifiable information ...; and	See 7.i (Ground 3) above.
[14.i] providing the produced healthcare information to report the characteristics of the group ... absent authorization	See 7.j (Ground 3) above.
[15] The computer readable storage devices of claim 14, wherein the healthcare information provided ... is in conformity with ... (HIPAA).	See 7.i (Ground 3) above.
[16] The computer readable storage devices of claim 14, wherein the request for healthcare information ... includes personally identifiable information	See 9 (Ground 3) above.
[17] The computer readable storage devices of claim 14, in which producing the requested healthcare information includes encrypting	See 10 (Ground 3) above.

Claim Clause	Dick in view of Landi and Murphy Ground
[18] The computer readable storage devices of claim 14,... identifying at least a minimum number of corresponding tokens.	See 11 (Ground 3) above.
[19] The computer readable storage devices of claim 14, in which the healthcare data represents medical related information	See 13 (Ground 3) above.

7. CONCLUSION

As demonstrated above, a reasonable likelihood exists that the Challenged Claims are unpatentable. Ex. 1003, ¶¶273-74. Accordingly, Petitioner respectfully requests *inter partes* review of the Challenged Claims.

Date: November 22, 2023

Respectfully submitted,

By: /s/Peter Shapiro
Peter Shapiro (Reg. No. 43,107)
Nicholas D. Marcello (Reg. No. 77,182)
PShapiro@Venable.com
NDMarcello@Venable.com
VENABLE LLP
151 W. 42nd Street
New York, NY 10036

T: 212-307-5500
F: 212-307-5598

Justin Oliver (Reg. No. 44,986)
JOliver@Venable.com
VENABLE LLP
600 Massachusetts Avenue, NW
Washington, D.C. 20001
T: 202-721-5423
F: 202-344-8300

Michael Sandonato (Reg. No. 35,345)
MSandonato@Venable.com
VENABLE LLP
2049 Century Park East, Suite 2300
Los Angeles, CA 90067
T: (310) 229-9900
F: (310) 229-9901

Attorneys for Petitioner Datavant, Inc.

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), I hereby certify that the foregoing Petition for *Inter Partes* Review contains 13,953 words as measured by the word processing software used to prepare the document, in compliance with 37 C.F.R. § 42.24(a).

DATED: November 22, 2023

Respectfully submitted,

By: /s/Peter Shapiro
Peter Shapiro (Reg. No. 43,107)
PShapiro@Venable.com
VENABLE LLP
151 W. 42nd Street
New York, NY 10036
T: 212-307-5500
F: 212-307-5598

CERTIFICATE OF SERVICE

I hereby certify that true and correct copies of the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 9,118,641 and accompanying exhibits were served on November 22, 2023 via USPS EXPRESS MAIL to the following address:

Correspondence Address of Record for U.S. Patent No. 9,118,641
FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN
UNITED STATES

Courtesy Copies Sent to Patent Owner's Litigation Counsel of Record in *Milliman, Inc. v. Gradient A.I. Corp.*, No. 1:21-Cv-10865-NMG (D. Mass.)

Christopher Centurelli
christopher.centurelli@klgates.com
K&L GATES LLP
State Street Financial Center
One Lincoln Street
Boston, MA 02111
Telephone: (617) 261-3100
Facsimile: (617) 261-3175

Christopher Dillon
dillon@fr.com
Fish & Richardson P.C.
One Marina Park Drive
Boston, MA 02210
Telephone: (617) 542-5070

Noah C. Graubart
graubart@fr.com
Joseph R. Dorris
dorris@fr.com
Fish & Richardson P.C.

1180 Peachtree Street NE
21st Floor
Atlanta, GA 30309
Telephone: (404) 892-5005

DATED: November 22, 2023

Respectfully submitted,

By: /s/Peter Shapiro
Peter Shapiro (Reg. No. 43,107)
PShapiro@Venable.com
VENABLE LLP
151 W. 42nd Street
New York, NY 10036
T: 212-307-5500
F: 212-307-5598