

Filed on behalf of: Datavant, Inc.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DATAVANT, INC.
Petitioner

v.

VIGILYTICS LLC
Patent Owner

IPR2024-00226
U.S. Patent No. 9,118,641 B2

PETITIONER'S REPLY

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Definition of a POSA.....	2
III.	Ground 2: Evenhaim in view of Settimi.....	2
	A. The Teaching of the References.....	3
	1. Evenhaim	3
	2. Settimi	3
	B. Vigilytics Improperly Limits Settimi to One Type of Query and Fails to Account for Evenhaim’s Undisputed Query	4
	C. The Combination Does Not Violate an Evenhaim “Preference”	6
	D. The Proposed Combination Does Not Violate HIPAA	8
	1. Safe Harbor Provision.....	9
	2. The Business Associate Exception	11
	3. Well Known Methods Existed to Prevent Vigilytics’ Hypothetical Attack	12
IV.	Ground 1 –Evenhaim.....	14
	A. Evenhaim Suggests Producing Tokens	14
	B. Whether tokenization would be needed in Evenhaim.....	16
	C. There is no “teaching away” from agglomerated data or token matching	17
V.	Ground 3: Dick and Landi	18
	A. The Teaching of the References.....	18
	1. Dick.....	18
	2. Landi	18
	B. A POSA would be motivated to combine Dick and Landi	18

C.	The Proposed Combination Discloses an Encryption Server for Producing Tokens for Individuals	20
D.	Vigilytics’ Argument Does Not Address the <i>Combination</i>	22
E.	Vigilytics Misconstrues Dr. Clark’s Testimony	23
VI.	Ground 4: Murphy	24
A.	Murphy Checks for a Minimum Number Before Producing Healthcare Information	24
B.	Murphy Does not Reject De-Identification.....	25
C.	A POSA Would Understand Murphy Blocks Queries.....	26
VII.	Conclusion	26

Cases

<i>Bayer Pharma AG v. Watson Labs., Inc.</i> , 874 F.3d 1316, 1328 (Fed. Cir. 2017)	17
<i>DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.</i> , 567 F.3d 1314 (Fed. Cir. 2009)	6, 26
<i>Elekta Ltd. v. ZAP Surgical Sys., Inc.</i> , 81 F.4th 1368 (Fed. Cir. 2023)	6
<i>Gen. Access Sols., Ltd. v. Sprint Spectrum L.P.</i> , 811 F. App'x 654 (Fed. Cir. 2020)	13
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	5
<i>ZUP, LLC v. Nash Mfg., Inc.</i> , 896 F.3d 1365 (Fed. Cir. 2018)	5

Statutes

45 C.F.R. § 164.514	9, 10, 19
---------------------------	-----------

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.
1014	Transcript of the Deposition of Aviel D. Rubin
1015	Reply Declaration of Dr. Paul Clark

Exhibit Number	Description
1016	<i>Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule</i> , U.S. Department of Health and Human Services, available at https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html
1017	Charles Safran, et al., <i>Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper</i> , 14 JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION (2007)
1018	William Landi, Ph.D & R. Bharat Rao, Ph.D, <i>Secure De-identification and Re-identification</i> , AMIA SYMPOSIUM PROCEEDINGS, p. 905 (2003)
1019	<i>May a covered entity share protected health information directly with another covered entity's business associate?</i> , U.S. Department of Health and Human Services, available at https://www.hhs.gov/hipaa/for-professionals/faq/241/when-is-a-health-care-provider-a-business-associate/index.html
1020	<i>To Whom Does the Privacy Rule Apply and Whom Will It Affect?</i> , U.S. Department of Health and Human Services, available at https://privacyruleandresearch.nih.gov/pr_06.asp
1021	37 C.F.R. § 160.103
1022	Provos & Mazieres, <i>A Future-Adaptable Password Scheme</i> , Proceedings of the FREENIX Track: 1999 USENIX Annual Technical Conference
1023	Morris & Thompson; <i>Password Security: A Case History</i> , 22 COMMUNICATIONS OF THE ACM 11 (1979)
1024	U.S. Pat. No. 7,668,820

I. Introduction

Vigilytics' Patent Owner Response ("POR") confirms that the claimed subject matter has long been known. The POR's Overview section explains that the purpose of the claimed system is to de-identify personal identifying information ("PII") so that it can be searched by, *e.g.*, insurance companies, without authorization from patients. However, that is what the federal rules for implementing HIPAA require and what the prior art teaches. The claims simply summarize what a POSA would (and did) do to comply with pre-existing laws for de-identification under HIPAA.

Tellingly, Vigilytics implies that the claimed subject matter is more similar to older designs that used centralized databases with de-identified medical records, as compared to one alternative option discussed in Evenhaim. That argument confirms that the claims recite well-known methods of aggregating healthcare records for querying. Interestingly, in view of the centralized, de-identified databases in the prior art, Vigilytics alleges that such designs risk bad actors trying to reverse engineer patient identities and thus, in Vigilytics' view, violate HIPAA. But that contradicts explicit statements in the prior art that such designs *are* HIPAA compliant.

Significantly, Vigilytics' expert confirmed that both the '641 patent and Settini (Ground 2) describe systems that use centralized databases that store de-identified patient records for searching. EX1014, 39:2-12, 20:22-23:13, 93:16-

95:22. Consequently, and because Vigilytics offers little rebuttal to Ground 2, Datavant begins with Ground 2 below.

II. Definition of a POSA

Vigilytics generally agrees with the Petition’s definition of a POSA, but asserts that the POSA would have had even more knowledge about medical databases and the manner of operating the same to comply with HIPAA. POR, 11-12. This strengthens the Petition inasmuch as the POSA would be even more sophisticated with respect to HIPAA compliance. EX1015, ¶7.

III. Ground 2: Evenhaim in view of Settimi

Vigilytics offers faint opposition to Ground 2. First, Vigilytics attempts to limit Ground 2 to only the exemplary queries in Settimi. This fails to appreciate the POSA’s level of skill (made more advanced by Vigilytics’ definition) and ignores that Ground 2 relies on *Evenhaim’s query*, which undisputedly meets the claim requirements. Second, Vigilytics alleges that Evenhaim must be limited to its alleged “preference” for searching raw datasets before de-identification. That argument mischaracterizes what constitutes preserving robust micro-level patient data (Evenhaim’s true preference) and improperly limits Evenhaim to one preferred embodiment.

A. The Teaching of the References

1. Evenhaim

Evenhaim describes searching for health records of specific patients. EX1015, ¶1; EX1005, 8:4-48, 6:56-67, 11:5-7, 13:62-14:3. Ground 2 relies, in part, on Evenhaim’s search for a specific list of patients in combination with Settimi. Pet., 36-40. Evenhaim explains its preference for maintaining and searching robust micro-level data (*e.g.*, specific diagnoses for a particular patient) as compared to prior art systems that provide lower resolution databases that compiled data. EX1005, 10:29-41, 12:36-67, 16:46-17:3, 7:32-58, 6:15-25, 17:28-40, Fig. 4. Specifically, Evenhaim discusses particular prior designs that did not allow for the searching of specific patient records. EX1005, 7:46-52.

2. Settimi

Settimi “generally relates to search and analysis of electronic medical record data.” EX1006, [0004], EX1015, ¶2. Settimi states that “[c]ertain embodiments provide systems and methods for searching electronic medical data to identify a pool of potential study participants.” EX1006, [0015]¹. Settimi is not limited to queries by pharmaceutical companies that seek study participants. *Id.*, [0030] (users can be “from companies that make . . . other products.”).

¹ Emphasis added throughout.

To facilitate searching, Settimi uses a centralized data warehouse that excludes patient identifiers, *i.e.*, PII, in accordance with HIPAA. *Id.*, [0009], [0017], [0027], [0035]; EX1015, ¶3. The PII is replaced with an encoded patient identifier (“EPID”). EX1006, [0038]; EX1014, 93:13-99:18. Unlike low-resolution databases, Settimi’s centralized warehouse “retain[s] clinically useful information about the patient.” *Id.*, [0038], [0040] (“dates of examination, documentation, diagnosis, prescription and lab test results”); EX1014, 89:14-90:6.

Vigilytics’ position is that Settimi limits queries to “characteristics” and that Settimi “fails to describe querying using EPIDs.” POR, 36. But, Settimi explicitly states that “[t]he user may *search by the EPID number.*” *Id.*, [0047], [0050] (“Thus, broader analysis of patient information may be allowed, while at the same time respecting patient privacy.”), [0051] (“Certain embodiments allow for patient information to be shared with interested parties without compromising patient privacy.”), [0071], [0073].

B. Vigilytics Improperly Limits Settimi to One Type of Query and Fails to Account for Evenhaim’s Undisputed Query

Regarding, for instance, claim elements [7.e]-[7.g], Vigilytics argues that Settimi is limited to queries only for patient “characteristics” (rather than for particular patients) and does not suggest searching by EPID (*i.e.*, token). POR, 36. This argument fails.

First, Ground 2 does not rely solely on Settimi for this element. Ground 2

references back to the application of Evenhaim (in Ground 1) for this element. *See* Pet., 37, 40-41. As Vigilytics’ expert admits, there is no dispute that Evenhaim describes a query for particular patients, through names or other identifying information. EX1014, 50:16-51:16, 72:11-73:20. Vigilytics ignores the Petition’s reliance on Evenhaim’s teaching of the type of query. The combination uses Settimi’s centralized database, which only identifies patients by tokens (EPIDs). Petition, 37, 40-41. The Petition relies on both Settimi and Evenhaim to suggest to a POSA that the query could be for specific patient records. *Id.* As discussed in the Petition, the patient names (or other identifying information) would be sent to the database in the form of tokens because tokens (“EPIDs”) are the only language Settimi’s centralized database would understand for identifying records. *Id.*; EX1015, ¶5.

Second, as discussed above, Vigilytics’ assertion that Settimi does not describe searching using EPIDs (POR, 36, 39-40) is false. EX1006, [0047] (“The user may search by the EPID, for example, and enter or select an EPID number to activate a search.”), [0050] (“broader analysis of patient information”), [0073]; EX1015, ¶¶4, 7. Thus, Vigilytics’ argument fails.

Additionally, Vigilytics’ arguments treat the POSA as an automaton with no ordinary creativity. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 420-21 (2007); *ZUP, LLC v. Nash Mfg., Inc.*, 896 F.3d 1365, 1373 n.2 (Fed. Cir. 2018) (explaining a

POSA is a person of ordinary creativity and applies art to solve known problems in an industry). It was well known at the time that there were varied interests in searching for patient data. EX1014, 47:12-50:15. While pharmaceutical companies had an interest in searching for any patients having a condition (to identify drug trial participants), insurance companies were known to search for specific groups of individuals to assess the risk of insuring the groups. *Id.*; see EX1007, [0003], [0008], [0025], [0037]. As Vigilytics' expert admits, a POSA would have understood that a searchable database containing health records would not be limited to conducting only one type of search. EX1014, 47:12-50:15. It would be illogical to accept that a POSA would limit Settimi to one embodiment that happens to focus on searching for patient conditions, particularly where Settimi states that its system is intended to be used by a wide array of companies (EX1006, [0030]) and Vigilytics' expert admits Settimi's disclosure in that regard is "very broad." EX1014, 102:3-103:8; 88:9-89:13.

C. The Combination Does Not Violate an Evenhaim "Preference"

First, preferences in prior art are just that, they are not exclusions as Vigilytics argues. POR, 39-40; EX1014, 83:3-8; see *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1327 (Fed. Cir. 2009) ("[a] reference does not teach away, however, if it merely expresses a general preference for an alternative"); *Elekta Ltd. v. ZAP Surgical Sys., Inc.*, 81 F.4th 1368, 1374 (Fed. Cir. 2023)

(explaining that obviousness does not require a particular combination be the preferred combination).

Second, the combination does not run contrary to Evenhaim's true preference. Evenhaim seeks to maintain a rich, searchable dataset, as compared to low-resolution datasets that have been stripped of valuable information. EX1005, 7:46-58; EX1015, ¶8. The lower resolution datasets were not preferred because they precluded analysis of "a predefined list of consumers participating in a health program." *Id.*, 16:46-17:3, 3:32-41. Specifically, those early databases did not maintain individual patient records, instead combining the information into a pool of data that was no longer linkable to any particular patient. EX1015, ¶¶6-9. Settimi's database preserves detailed medical records, while only tokenizing identifying information for those records to comply with HIPAA. EX1006, [0060]-[0061], [0063]. Consequently, the proposed combination would still permit the searching (using tokens) of a "predefined list" of patients to obtain the record for those patients, which is Evenhaim's goal. EX1015, ¶¶6-9. The combination simply achieves the goal using a centralized data warehouse, for which there are additional benefits addressed in Settimi. EX1006, [0060]; EX1014, 10:1-21, 80:22-81:22. Further, Vigilytics' expert agrees that the level of granularity for Settimi's database would be up to the designer. Ex1014, 87:8-88:8, 96:1-13.

Vigilytics' argument that Settimi's database lacks the original raw data (due

to de-identification) is also misguided in view of Evenhaim’s explicit disclosure. Evenhaim describes searches in which the patient is identified other than by his/her name. EX1005, 8:30-43 (“the aggregator may accept a query that includes . . . a list of names or a combination of a few fields that together can allow for identification;” “the parameter list may even include specific individuals by name or ID or the like[.]”). Thus, Evenhaim acknowledges that original, unaltered patient names are not required to achieve its goal. Also, Evenhaim acknowledges that the “micro-level records” that it seeks to maintain are not harmed by the removal of PII inasmuch as Evenhaim acknowledges the option of “*identity-free* micro-data.” *Id.*, 10:29-32, 12:36-52, Fig. 4 (“micro data”); EX1014, 61:17-67:2 (distinguishing micro-level data from physician level data); *see* EX1006, [0038], [0043].

Notably, regarding Evenhaim’s explanation that a search may use an ID rather than a name (EX1005, 8:30-43 (“name or ID or the like[.]”)), the construction of “token,” which Vigilytics does not dispute, is an “identifier.” *Pet.*, 8.

Thus, Vigilytics’ argument that Evenhaim “teach[es] away” (POR, 39-40) fails.

D. The Proposed Combination Does Not Violate HIPAA

While not actually raised in Ground 2, Vigilytics argues in response to Ground 1 that using keys for tokenization on both the aggregator side and data source side, in Evenhaim, would risk that a bad actor at the aggregator could reverse engineer

patient identities corresponding to records returned from the data source. POR, 25-26. Specifically, Vigilytics hypothesizes that a bad actor at Evenhaim’s aggregator, in using a key to encrypt (*e.g.*, tokenize) a patient’s identifying information, could save the tokens and original names in, *e.g.*, a table to attempt to look for the same tokens in the returned search results to determine which patients correspond to the records. Vigilytics’ speculative example does not undermine the fact that, as discussed below, a POSA would know how to use Evenhaim without violating HIPAA and the applied references intend to *achieve* HIPAA compliance. *See* EX1014, 33:12-34:4; EX1005, 2:5-26. The argument also ignores that a bad actor anywhere in the system could theoretically break a rule.

In any event, to the extent that Vigilytics may attempt to have the argument apply to Ground 2, it fails.

1. Safe Harbor Provision

Under 45 C.F.R. § 164.514(b)(2), the removal of identifying information by a covered entity renders the data no longer covered by HIPAA. *See* EX2006; EX1016, 9-11 (“safe harbor”); EX1014, 101:12-10:2; EX1006, [0009]. Once a covered entity, such as a doctor’s office, removes that information and provides it to a central database, there is no HIPAA violation in the disclosure and use of those de-identified records, absent *actual knowledge* the information could be used to identify patients. *See id.* Vigilytics appears to ignore this point or to assume a covered entity

would have actual knowledge of a hypothetical bad actor. EX1015, ¶¶10-15; *see* EX1005, 9:59-67 (“good conscience”).

Notably, Vigilytics’ own expert was unable to confirm “on the fly” what would, or would not, be a HIPAA violation, stating he would need to study the issue. EX1014, 121:22-122:9, 126:5-7, 115:15-117:15, 129:15-130:17; 71:4-72:5. Also, the credibility of Vigilytics’ expert is undermined by the fact that he expressed positions concerning HIPAA that are facially incorrect. He stated that the existence of *any* key to decrypt the tokenized identifying information would be a HIPAA violation. EX1014, 34:5-37:7, 41:1-14; 117:16-118:8. However, HIPAA rules *explicitly allow* for re-identification so long as the decryption key is kept confidential. EX2006, 45 C.F.R. 164.514(c); EX1016, 11-12. Thus, both Vigilytics’ and its expert’s assertions regarding HIPAA are not supported by the record.

Vigilytics and its expert also assert that use of a centralized database for searching tokenized records (as described in Settimi and Landi) would be inherently violative of HIPAA. POR, 25-27, 51-52, 58-59; Ex. 2001, 102, 113, 118, 159-161. But the applied references are all directed to *complying* with HIPAA. EX1008, 3:52-57 (“[S]ystems and methods according to the invention ... while maintaining compliance with regulations based on HIPAA for protecting personal privacy.”); EX1005, 14:56-67; EX1006, [0009], [0014], [0017], [0027]; EX1017, 3; *see infra* § V. Thus, Vigilytics’ assertions regarding HIPAA are again contradicted by the

record. Vigilytics offers no reason why a POSA would disregard those explicit teachings. Indeed, Vigilytics' expert admitted that (i) analyzing HIPAA compliance cannot be done on the fly, instead taking weeks to perform and (ii) even after his own review he was still not sure about whether certain matters he stated might be HIPAA violations, would truly be HIPPA violations. EX1014, 34:5-37:7, 121:22-122:9, 126:5-7. If, even now, Vigilytics' expert is unsure of these issues, it cannot be that a POSA reading explicit statements in the prior art regarding HIPAA compliance would reject the same, which, at base, is Vigilytics' position.

2. The Business Associate Exception

Under HIPAA, it is not a violation to use business associates to hold patient records, so long as there is an agreement in place. EX1021 (defining business associate), EX1020, 3; EX1016, 6. A covered entity can contract out certain functions to business associates so that those entities can handle protected healthcare data without any HIPAA violation. A POSA would readily understand that, *e.g.*, a centralized database and/or aggregator could be business associates of each other and/or a healthcare system (if they themselves are not covered entities). EX1015, ¶¶12-13. Indeed, an aggregator (as in Evenhaim) and a centralized database could be part of the same entity, (whether a covered entity or business associate of a covered entity), such that the business agreement would preclude any concern of a potential HIPAA violation by a rogue actor. See EX1017-1019; EX1015, ¶¶12-13;

EX1014, 25:13-28:17; 51:17-53:17. Vigilytics' expert admitted that there would likely be some business agreement between the aggregator in Evenhaim and a data source to which the aggregator sends the query. EX1014, 29:13-30:10 ("So I think in that hypothetical scenario it would be either a contractual agreement or just an understanding that the point of this encryption server is that it should not be sharing all of its information with the public."); EX1005, 5:12-28. A POSA would expect the use of agreements that require associates to maintain privacy, removing HIPAA concerns. EX1015, ¶¶10-13.

3. Well Known Methods Existed to Prevent Vigilytics' Hypothetical Attack

The idea of bad actors using a public key to encrypt a known identifier and then maintaining the identifier and encrypted version in correspondence to attempt to circumvent security measures has long been known in the field. Such an attack is known as a "plain text" attack (with "chosen" and "known" being the two types). EX1014, 42:10-47:11; EX1015, ¶¶14-15. Vigilytics' expert acknowledges these types of attacks have been known at least since the 1990s. *Id.* He also acknowledges that, since the 1990s, there have been known defenses. One such defense is a "salt," in which the encryption system adds random data to, *e.g.*, a token to block the usefulness of a lookup table. EX1014, 45:6-46:1, 25:13-28:17 ("[a] POSA would understand that it would apply known known security techniques"); EX1015, ¶¶14-15, EX1022, 5-6, EX1023, 597. Another is cypher block chaining, which ties pieces

of encrypted data together to make such attacks impractical. EX1014, 46:2-47:11. Both techniques were basic, known mechanisms for a POSA to guard against Vigilytics’ hypothetical attack, if it were a real concern. *Id.*

Additionally, Vigilytics criticizes the Petition’s explicit identification of another known method to block plain text attacks—namely, applying additional encryption before returning query results. POR, 25-26; Ex. 2001, ¶111². Specifically, Vigilytics offers only that Dr. Clark’s testimony on this point lacks corroboration. *Id.* First, neither Vigilytics nor its expert *dispute* the stated defense. Second, to the extent that corroboration is needed, *in addition* to Dr. Clark’s unrebutted testimony on this point, the same is discussed in, for example, U.S. Pat. No. 7,668,820. EX1024, 2:20-51, 5:26-61; EX1015, ¶15; *see also* EX1018 (“Study ID”).

Finally, Evenhaim explicitly discusses using an “escrow agent” on the

² It is difficult to ascertain what testimony from the declaration Vigilytics is relying upon because its analysis sections repeatedly cite to numerous paragraphs of EX2001. Ground 1’s analysis section repeats citation to “EX2001, 100-137” over 30 times, with no specific declaration cites. Consequently, Vigilytics reliance on the declaration should be entitled to little weight. *See Gen. Access Sols., Ltd. v. Sprint Spectrum L.P.*, 811 F. App’x 654, 658 (Fed. Cir. 2020).

aggregator side so that the key may not be known to the aggregator, thus further guarding against bad actors at the aggregator. EX1005, 12:63-66; *see* EX1008, 4:9-19 (“trusted broker”); EX1014, 132:5-21. Vigilytics’ expert admitted that such an agent could hold keys for encrypting and decrypting. EX1014, 51:17-53:17. In this regard, the very purpose of these systems, including Evenhaim, is so that the identity of the patient is “not knowable.” EX1005, 13:1-20. Thus, a POSA would understand that any one of several options could be used to protect privacy. *See id.*, 13:33-39 (explaining that encryption options are well known); EX1006, [0041].

IV. Ground 1 –Evenhaim

A. Evenhaim Suggests Producing Tokens

Vigilytics tries to limit the encryption described in Evenhaim to general encryption for data transmission. POR, 13-14, 16. However, Evenhaim describes different encryption for the patient list and the overall query message, such that the encryption/tokenization of patient names differs from the transmission encryption. EX1005, 13:33-43, 14:3-13. Further, Evenhaim states that *parts of the parameter list* may be encrypted. EX1005, 8:43-48, 12:24-34 (explaining that encryption can happen anywhere in the system); EX1014, 79:5-20, 53:18-54:20 (admitting Evenhaim’s hash equates to tokenization), 37:8-38:9. Thus, Evenhaim suggests that, separate from general transmission encryption, parts of the list, such as patient names, may be separately encrypted. This is consistent with the testimony of Dr.

Clark quoted by Vigilytics. POR, 17. It also explains why Evenhaim describes decryption at the data source—specifically, the decryption at the data source is for the general transmission encryption. EX1015, ¶¶16-17.

Vigilytics’ expert acknowledged Evenhaim’s teachings on this point and even admitted that the enhanced encryption for parts of the parameter list (which he calls “super encryption”) would remain *after* the transmission encryption is decrypted. EX1014, 74:14-79:3 (“the transmission encryption is peeled off, but the super encryption remains”; “[s]o I think that this language is very broad and it could mean that certain types of fields aren’t encrypted and others are”), 84:5-20. This supports that Evenhaim’s encryption of parts of the parameter list suggests tokenization. EX1015, ¶¶17-18.

Moreover, the purpose of HIPAA that Evenhaim is trying to match is de-identification through the encryption of PII. Evenhaim does not limit where that happens. EX1005, 11:43-46 (functions can be reversed). Vigilytics’ argument is that it would happen in only one place in Evenhaim—after the searching—which is contrary to Evenhaim’s statement on this point. *Id.*, 8:43-48, 12:24-34. And, Evenhaim acknowledges that searching centralized databases that have already been de-identified was known long before Evenhaim. Thus, Vigilytics’ argument is essentially that its claims replicate *older* designs more than one optional advancement described in Evenhaim.

Also, Vigilytics' own expert acknowledges that systems such as Evenhaim's employ standard formatting to make queries workable, such that the search for "Joe Smith" also captures "Joseph Smith." EX1005, 8:30-56, 10:37-41. It is undisputed that tokenization provides a method for accomplishing the same. In fact, as discussed above, Evenhaim describes that the query can use an "ID" or the like (*i.e.*, a token), instead of a name. EX1005, 8:30-43; EX1014, 40:8-18 (agreeing with construction of "token"). Indeed, it was long known that tokenizing an identity using, *e.g.*, part of the person's name, the person's DOB, and part of the person's SSN achieves Evenhaim's goal. See EX1008, 5:2-19; EX1005, 8:30-34 ("a combination of a few fields that together can allow for identification"), 13:1-12. For these reasons, a POSA would understand Evenhaim's encryption of part of the parameter list (and combining of fields) to suggest tokenization.

Also, while Vigilytics alleges that a search at the data source cannot be of tokenized data because Evenhaim says that the search "may" involve name matching through fuzzy logic (POR, 29), the use of "may" confirms Evenhaim is not so limited. EX1005, 9:45-51, 8:30-43, 13:33-43.

B. Whether tokenization would be needed in Evenhaim

Vigilytics argues that there would be no need to de-identify the patient list or query through encryption. POR, 23-29. This squarely contradicts Evenhaim, which specifically describes encrypting both (using higher encryption levels for the patient

list), as discussed above. Thus, the question is simply whether it would have been obvious to perform such de-identification of PII (which is part of the parameter list), based on Evenhaim's explicit disclosure of encrypting such information, pre-transmission to the data sources. Vigilytics' argument is that a POSA would not find it obvious to do exactly what Evenhaim says to do—performing encryption on the aggregator side. Moreover, the approach that Vigilytics accuses of being “nonsensical” (POR, 23-29) is what the '641 patent describes and claims, making its argument suspect at best. EX1001, Fig. 3, claim 7; EX1014, 30:13-34:4; EX1005, 12:24-34.

C. There is no “teaching away” from agglomerated data or token matching

There is also no “teach[ing] away” from agglomerated data or token matching. POR, 27, 34, 1. In Evenhaim, there is merely a statement that low resolution agglomerated data is not robust for some applications. EX1005, 3:32-41, 5:4-7, 1:38-50. A POSA would have understood that agglomerated data can be as robust as the designer intends, as discussed above. *Bayer Pharma AG v. Watson Labs., Inc.*, 874 F.3d 1316, 1328 (Fed. Cir. 2017) (explaining that a preferred embodiment or better does not support a finding of teaching away).

V. Ground 3: Dick and Landi

A. The Teaching of the References

1. Dick

It is undisputed that Dick describes querying de-identified medical information for a group of individuals. EX1007, [0024]-[0025]; EX1014, 114:2-115:9; EX1015, ¶19. Ground 3 relies on Dick’s search for a specific group of humans. Pet., 51-55. While Dick recognizes HIPAA restrictions and the benefits of de-identification, it generally “contemplates” “methods and processes” for the same, without directing specific processes. EX1007, [0046]-[0047]; *see* EX1014, 111:7-113:6; EX1015, ¶19.

2. Landi

Landi describes how organizations can de-identify patient records using an encrypted ID, *i.e.*, token. EX1015, ¶20. Those tokens enable patient records to be located and released to third-party entities without revealing patient identities. EX1008, 1015-31, 14:26-29; EX1015, ¶20. Landi does allow for the re-identification of records, but only at the places where de-identification occurred (*e.g.*, covered entities). EX1008, 7:22-30, 2:5-49, 5:32-47, 8:16-18, 8:60-63.

B. A POSA would be motivated to combine Dick and Landi

Vigilytics argues that the Petition fails to demonstrate a motivation to combine Dick and Landi because Dick already provides de-identification methods. POR, 48-49. The paragraph cited by Vigilytics merely recites the two requirements that are in

the HIPAA statutes: (1) remove PII or (2) statistical obfuscation. *Compare* EX1007, [0045] *with* EX2006, 45 C.F.R. § 164.514. Dick is only telling a POSA what must be done in general terms. It is not endorsing a particular technical operation. EX1015, ¶21.

The other paragraphs from Dick that Vigilytics cites, [0046]-[0047], do nothing more than discuss the goals and benefits of de-identifying. EX1007, [0046] (describing the benefits of de-identification in medical research), [0047] (describing a way to find patients for a study). Again, no technical techniques are described. The testimony from Dr. Clark cited by Vigilytics does not change this understanding. POR, 48-50. Vigilytics' question only asked whether a POSA would be able to de-identify without going beyond Dick. That a POSA would have been well-versed in de-identification options does not affect that a POSA would have had reason to elect a specific methodology, as described in Landi. EX1015, ¶¶21-22. As Vigilytics admits, simple de-identification is not the issue here. POR, 60 (“[T]he claims are not directed to mere ‘token matching’ or ‘de-identification.’”). A POSA would have found it obvious to select any one of several technological methods, including Landi's option.

Also, a method for de-identifying was not the only reason given for combining Dick and Landi. The Petition also relies upon on Landi's “central database” design as an option. Petition, 53. This reason is not contested in the POR.

Vigilytics also contends that a POSA would not turn to Landi because it is allegedly not HIPAA compliant. POR, 51-52. The general failure of this analysis is addressed above with respect to Ground 2. Moreover, Landi explicitly states that its design presents “no HIPAA issues” and that its goal is HIPAA compliance. EX1008, 3:52-57, 8:38-55; EX1014, 115:15-117:15. Thus, Vigilytics’ argument amounts to asking the Board to accept that a POSA would ignore Landi’s explicit teachings and/or would implement the combination in a non-complaint way, in violation of Landi’s teachings. At base, Landi describes a tokenization method for a centralized, de-identified database, as Vigilytics’ expert admits (EX1014, 131:1-133:10), and has as its goal HIPAA compliance. EX1008, 3:52-57, 8:38-55; EX1015, ¶23.

C. The Proposed Combination Discloses an Encryption Server for Producing Tokens for Individuals

Vigilytics asserts that there is no need for the requester’s server to provide tokens rather than patient names. POR, 56. But, this argument relies on a hypothetical posed to Dr. Clark and cites his testimony out of context. POR, 56. Reviewing the context of the question shows that Dr. Clark was not analyzing Dick, Landi, or the combination of Dick and Landi. The testimony Vigilytics cites relates to a discussion concerning Evenhaim. EX2002, 57:16-58:3, 57:20-21 (Dr. Clark explaining he needs to look at the *specific example* to fully answer the question). Thus, Vigilytics is improperly attempting to apply Dr. Clark’s testimony concerning Evenhaim, to the combination of Dick and Landi. In any event, the argument fails

for reasons addressed above with respect to Evenhaim. Also, the argument ignores that the centralized database in Landi would not know patient names, inasmuch as the records are already de-identified, as Vigilytics' expert admits. EX1014, 131:1-132:4; EX1008, 7:3-38.

Vigilytics also argues that no encryption server is disclosed in the combination because Landi only describes encryption at the patient center, so it is allegedly impermissible hindsight bias to implement it at Dick's requester's server. POR, 57-58. This is incorrect and overly restrictive based on the teachings of Landi. As discussed above, Landi's central database stores de-identified records in which PII is replaced with an encrypted ID. EX1008, 4:40-46, 11:23-29. A POSA applying Dick's search for patient records in Landi's central database would understand that the manner of finding the same would be through searches for encrypted IDs, *i.e.*, tokens. Thus, this is not impermissible hindsight bias, it is a POSA's simple understanding that, for a centralized database that only has encrypted IDs, identifying patient records would need to use queries with encrypted IDs. This is a simple manner of understanding that a database can be subject to various types of queries, as Vigilytics' own expert acknowledged. EX1014, 47:12-50:15; *see* EX1009, 556.

Additionally, the POR's own figures show that the encryption in Landi is not restricted to only patient centers. For example, the surveillance system has an

encryption system and Landi explains that “the central data processing system (30) and the central surveillance system (50) may be combined into one system.” EX1008, 7:65-8:4; POR, 55. Thus, Vigilytics is incorrect that Landi only contemplates encryption at the patient centers. *Id.*, 9:16-19. A POSA would understand that encryption/tokenization can occur where useful, including at Dick’s requester server.

Finally, Vigilytics also claims that the combination would present a HIPAA violation because it would release to the requester server information sufficient to correlate de-identified patient records with the patients, *i.e.*, a plain text attack. This argument fails for reasons discussed above with respect to Ground 2.

D. Vigilytics’ Argument Does Not Address the *Combination*

Vigilytics also contends that the combination does not render certain elements obvious because Landi does not match tokens. POR, 59-62.

First, the deficiencies in this argument are already addressed above. Second, Vigilytics is wrong that Landi does not contemplate the ability to search by identifying tokens. Landi explicitly states that identifying patient data is replaced in the patient record and maintained in database tables “wherein the patient data elements are known a priori and can readily be searched.” EX1008, 11:52-63; *see also* cl. 12 (mapping an Encrypted ID to a Study ID). Vigilytics ignores this disclosure. The portions cited by Vigilytics (POR, 60-61) show, in combination with

the above disclosure, that Landi at least suggests to a POSA that Landi was concerned with the ability to maintain the usefulness of the encrypted IDs when processing and searching for data. *Id.*, 8:23-55,11:23-29. In other words, a POSA would understand Landi’s teachings about maintaining consistency in creating encrypted IDs would enable searching for specific patient records. EX1008, 11:23-29 (“[T]he process preserves patient uniqueness to enable the same patient to be recognized at different collection times.”).

Regardless, the combination relies upon Dick for the well-known idea of searching for specific patient records, which a POSA would understand could only be performed in Landi’s database using the encrypted IDs. While Vigilytics also argues that Landi does not teach querying a central database (POR, 61-62), the argument again ignores the reliance on Dick. The Petition does not solely rely on Landi for querying, it also refers to Dick’s searches. Pet., 60-63; EX1003, ¶222. Also, Landi *does* disclose the ability to search database records. EX1008, 11:52-63 (“[P]atient data is typically maintained in database tables . . . and can readily be searched.”).

E. Vigilytics Misconstrues Dr. Clark’s Testimony

In a last-ditch effort, Vigilytics misconstrues Dr. Clark’s testimony to assert that produced healthcare information in Dick and Landi is not absent PII. POR, 62-63. Dr. Clark merely stated that returned information in Landi may include the

encrypted ID. EX1015, ¶24. That does not mean that “PII is available in the produced healthcare information.” POR, 63. The encrypted ID would need to be decrypted to reveal the identity of the individual. Landi explains that only encrypting entities can decrypt IDs. EX1008, 3:42-48, 6:61-65, 7:22-30, 10:32-45, 11:13-17. Therefore, Vigilytics argument fails inasmuch as a returned record would be associated with only the encrypted ID, with no ability to decrypt it. EX1015, ¶24.

VI. Ground 4: Murphy

A. Murphy Checks for a Minimum Number Before Producing Healthcare Information

Murphy is concerned with preventing the production of protected information (*e.g.*, when too few records will be returned). EX1014, 134:8-137:16 (“so that one can’t see what the actual values are”); EX1015, ¶25. Murphy describes performing a check to ensure at least a minimum number of records were identified. EX1009, 553. If that minimum number is not met (*e.g.*, 3), in the example, a message is provided that says “<3.” *Id.* That does not answer the query posed (*e.g.*, specifically stating the number of hits). The POR seems to agree. POR, 67 (“rather than returning an absolute value”). Yet, Vigilytics asserts that because Murphy’s system “returns a numerical result” it must be understood that “the query is still answered.” POR, 66-67. That argument fails. Murphy’s example query asks for the specific number of patients with, *e.g.*, a particular condition. EX1009, 552-553. The answer to that

question is *not* answered when the answer would be below some selected threshold. EX1015, ¶26.

Vigilytics also improperly isolates Murphy from its combination with Dick and Landi to argue that Murphy is only concerned with returning a number, as opposed to patient records. Though Murphy may, in its example, return the number of records rather than the records themselves, the Dick-Landi combination returns records, as discussed above. Murphy is relied upon simply to teach that, for privacy reasons, a POSA would understand that a system would preferably set a minimum number of patients to guard against a requester matching a particular patient to the query/response. EX1009, 552-53; EX1015, ¶27. That concept is applicable regardless of the nature of the query. Indeed, Murphy explains that its concept is not limited to the type of query, and Vigilytics’ expert agreed. EX1014, 137:17-138:22 (“those examples are not limiting, it could be other things, too”); EX1009, 556 (“does not limit the logic of the query”).

B. Murphy Does not Reject De-Identification

Murphy recognized that de-identification alone may not be sufficient to protect privacy, so Murphy added a tool applying principles based on data obfuscation. EX1009, 553 (explaining that de-identification is a “good start”). Murphy’s concern was that a targeted search-type attack could still reveal the identity of an individual if the parameters of the search were narrow enough.

Contrary to Vigilytics' position (POR, 68), Murphy does not reject de-identification, but supplements it. *Id.* Murphy contains no statements that disparage or teach away from de-identification. *See DePuy*, 567 F.3d at 1327.

C. A POSA Would Understand Murphy Blocks Queries

Vigilytics' argument that Murphy does not suggest blocking queries, is incorrect. A POSA would understand Murphy to be generally about preventing the return of too few hits, such that a requester could identify a particular patient, and, specifically, not truly answering such queries. This is akin to a warning or error message. EX1015, ¶26. To the extent that Vigilytics is intending to present such an argument, a POSA would understand that the precise point of the blockage is simply a design choice. EX1015, ¶28. Indeed, Murphy's stated concern is a user trying to identify one individual through *narrowing* parameters. EX1009, 552-53. Murphy's goal is to prevent that outcome, regardless of the type of query or manner of attack by the user.

VII. Conclusion

For these reasons, the Challenged Claims are unpatentable.

DATED: December 11, 2024

Respectfully submitted,

Justin J. Oliver
Justin J. Oliver
VENABLE LLP
600 Massachusetts Avenue, NW

Washington, D.C. 20001
Telephone: 202-721-5423
Facsimile: 202-344-8300
Email: JOliver@Venable.com

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

I hereby certify that this Reply complies with the word count limitation of 37 C.F.R. § 42.24(a)(1) because the Reply contains a total of 5,595 words. This total excludes the cover page, signature block, and the parts of the petition exempted by 37 C.F.R. § 42.24(a)(1).

DATED: December 11, 2024

Justin J. Oliver
Justin J. Oliver
VENABLE LLP
600 Massachusetts Avenue, NW
Washington, D.C. 20001
Telephone: 202-721-5423
Facsimile: 202-344-8300
Email: JOliver@Venable.com

CERTIFICATE OF SERVICE

The undersigned certifies that a complete copy of this Reply and all Exhibits and other documents filed together with this Reply were served on the Patent Owner at:

IPR25412-0020IP1@fr.com
PTABInbound@fr.com
axf-ptab@fr.com
barclay@fr.com
nstephens@fr.com

DATED: December 11, 2024

Justin J. Oliver
Justin J. Oliver
VENABLE LLP
600 Massachusetts Avenue, NW
Washington, D.C. 20001
Telephone: 202-721-5423
Facsimile: 202-344-8300
Email: JOliver@Venable.com