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

IPR2024-00307
U.S. Patent No. 9,965,651

PETITIONER'S REPLY

TABLE OF CONTENTS

I. Introduction 1

II. Definition of a POSA 2

III. Ground 2: Evenhaim, Settimi and Murphy 2

A. The References 2

1. Evenhaim 2

2. Settimi 3

3. Murphy 4

B. Vigilytics Improperly Limits Settimi to One Query Type and Ignores Evenhaim 4

C. The Combination Does Not Violate an Evenhaim "Preference" 6

D. Vigilytics' Alleged HIPAA Problem is Illusory 8

1. Escrow Agent 10

2. Well-Known Cryptographic Methods 10

3. HIPAA Rules 11

IV. Ground 1 –Evenhaim and Murphy 13

A. Evenhaim Suggests Producing Tokens 13

B. Whether Tokenization Would Benefit Evenhaim 15

C. There is No "Teaching Away" 15

D. Evenhaim and Murphy Suggest Determining Minimums According to a Privacy-Preserving Rule 15

V. Ground 3: Dick, Landi and Murphy 18

A. The References 18

1. Dick 18

2. Landi 18

B. Motivation to Combine Dick, Landi and Murphy 18

C. The Combination Suggests Producing Tokens for Individuals 21

D. Vigilytics' Argument Does Not Address the *Combination* 22

E. Vigilytics Misconstrues Dr. Clark's Testimony 23

F. Murphy Teaches Using Minimums to Block Attacks.....24

G. A POSA Would Understand Murphy Blocks Queries.....25

H. Vigilytics Misconstrues Murphy.....25

VI. Conclusion 26

Cases

DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc., 567 F.3d 1314 (Fed. Cir. 2009) 6

ZUP, LLC v. Nash Mfg., Inc., 896 F.3d 1365 (Fed. Cir. 2018) 6

Statutes

45 C.F.R. § 164.514 ..... 12, 18

Exhibit List

Exhibit Number	Description
1001	U.S. Patent No. 9,965,651(the "'651 Patent")
1002	File History of U.S. Patent No. 9,965,651
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, *A Security Architecture for Query Tools used to Access Large Biomedical Databases*, 2002 AMIA Annual Symposium Proceedings, 552 (2002) ("Murphy")
1010	*Milliman, Inc. v. Gradient A.I. Corp.*, No. 1:21-Cv-10865-NMG (D. Mass.), Dkt. 108.
1011	*Credit Card Security: The Best Way to Secure Data is Not to Store the Data* (Hospitality Upgrade, Summer 2008, www.hospitalityupgrade.com)
1012	Jennifer G. Steiner, B. Clifford Neuman, and Jeffrey I. Schiller, *Kerberos: An Authentication Service for Open Network Systems*, Winter 1988 Usenix Conference (1988).
1013	Declaration of Sylvia Hall-Ellis, Ph.D.
1014	Transcript of the Deposition of Aviel D. Rubin from related IPR2024-00226
1015	Reply Declaration of Dr. Paul Clark

Exhibit Number	Description
1016	*Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, 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., *Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper*, 14 JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION (2007)
1018	<RESERVED>
1019	<RESERVED>
1020	*To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, 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, *A Future-Adaptable Password Scheme*, Proceedings of the FREENIX Track: 1999 USENIX Annual Technical Conference
1023	Morris & Thompson; *Password Security: A Case History*, 22 COMMUNICATIONS OF THE ACM 11 (1979)
1024	U.S. Pat. No. 7,668,820
1025	Transcript of the Deposition of Aviel D. Rubin

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 de-identifying personal identifying information ("PII") so that it can be searched without patient authorization. That is precisely what the prior art teaches. Thus, the claims simply summarize known privacy techniques. *See* EX1025, 9:10-11:4.

Tellingly, Vigilytics implies that the claimed subject matter is more similar to older designs that used centralized databases with de-identified records, as compared to an alternative discussed in Evenhaim. But that confirms the obviousness of the claims. Interestingly, concerning de-identified databases in the prior art, Vigilytics alleges that such designs risk bad actors trying to reverse engineer PII and, thus, purportedly could violate HIPAA. That argument contradicts the references' explicit statements that their designs are for *complying* with HIPAA. It also fails to acknowledge that the '651 Patent's design would be equally at risk to bad actors.

Significantly, Vigilytics' expert confirmed that both the '651 Patent and Settimi (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.[1] Because Vigilytics offers little rebuttal to Ground 2, Datavant begins with that ground.

II. Definition of a POSA

Vigilytics asserts that the POSA would have been more knowledge about medical databases and the manner of operating the same to comply with HIPAA. POR, 11-12. This sophisticated POSA strengthens the Petition. EX1015, ¶7.

III. Ground 2: Evenhaim, Settimi and Murphy

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 level and ignores Ground 2's reliance on *Evenhaim's query*, which undisputedly meets the claim requirements. Second, Vigilytics alleges that Evenhaim must be limited to its alleged "express preference" for searching raw datasets (before de-identification). That argument mischaracterizes Evenhaim's mere preference for "high resolution" data.

A. The References

1. Evenhaim

Evenhaim describes searching for records of specific patients. EX1015, ¶8; EX1005, 8:4-48, 6:56-67, 11:5-7, 13:62-14:3. Ground 2 relies on Evenhaim's search

[1] Deposition from related IPR2024-00226.

for specific patients in combination with Settimi. Pet., 40-46. Evenhaim prefers searching micro-level data (*i.e.*, patient level) as compared to prior systems with lower resolution databases that did not contain specific patients' records. EX1005, 10:29-41, 12:36-67, 16:46-17:3, 7:32-58, 6:15-25, 17:28-40, Fig. 4.

2. Settimi

Settimi "generally relates to search and analysis of electronic medical record data." EX1006, [0004], EX1015, ¶9. Settimi states that "*[c]ertain embodiments* … search[] … to identify a pool of potential study participants." EX1006, [0015][2]. Settimi is not limited to such queries. *Id.*, [0030] ("companies that make . . . other products."), [0061].

For searching, Settimi uses a centralized database that excludes PII, in accordance with HIPAA. *Id.*, [0009], [0017], [0027], [0035]; EX1015, ¶10. The PII is replaced with an encoded patient identifier ("EPID") that is created using a hash function (or "[o]ther methods") – the same tokenization example in the '651 Patent and Evenhaim. EX1006, [0038], [0041] ("hashes"); EX1001, 6:59-7:4; EX1006, 12:36-42; EX1014, 93:13-99:18; EX1025, 31:21-32:18. Unlike low-resolution databases, Settimi's database "retain[s] clinically useful information about the patient." *Id.*, [0038], [0040] ("documentation, diagnosis, …"); EX1014, 89:14-90:6.

[2] Emphasis added throughout.

Settimi states that "[t]he user may *search by the EPID number*." *Id.*, [0047], [0050] ("broader analysis of patient information"), [0051], [0071], [0073]. Settimi also describes searches of the user's own design. *Id.*, [0061].

3. Murphy

Murphy blocks identification of patients through targeted searches. EX1014, 134:8-137:16; EX1015, ¶36; EX1025, 51:15-53:5. Specifically, Murphy's design uses minimums to ensure a sufficient pool of results. EX1009, 553.

B. Vigilytics Improperly Limits Settimi to One Query Type and Ignores Evenhaim

Regarding, *e.g.*, claim elements [7.e]-[7.g], Vigilytics argues that Settimi is limited to queries for only patient "characteristics" (rather than for particular patients) and does not suggest searching by the token (*e.g.*, EPID). POR, 41-44. This argument fails.

First, Ground 2 does not rely solely on Settimi for this element, instead referencing the application of Evenhaim in Ground 1. Pet., 38-41, 45-48. Vigilytics' expert admits that Evenhaim describes querying particular patients. EX1014, 50:16-51:16, 72:11-73:20. Yet, Vigilytics ignores the Petition's reliance on Evenhaim. The combination uses Settimi's centralized database, which only identifies patients by tokens (created by hash functions) and relies on *both* Settimi and Evenhaim to suggest a query for specific patient records in the database. Pet., 38-41, 45-48. As discussed in the Petition, the patient records would be queried using tokens because

tokens (*e.g.*, "EPIDs") are the only language Settimi's centralized database understands for identifying records. *Id.*; EX1015, ¶¶11-12. Further, Evenhaim teaches formatting the names provided by users into terminology mutually agreed to by the aggregator and the source entities, including "name or ID or the like[]." EX1005, 8:30-43, 49-55; EX1025, 31:7-19 (explaining that a token equates to a person). Thus, Evenhaim's query would be formatted to match a token design used by Settimi's database.[3]

Second, as discussed above, Vigilytics' assertion (POR, 41-44) that Settimi does not describe searching using EPIDs fails. EX1006, [0047] ("The *user may search by the EPID*, for example, and enter or select an EPID number to activate a

[3] Although not presenting claim constructions for any terms, it appears that Vigilytics may allege that the claimed tokens must be limited to only one-way encryption (hash functions). EX1025, 13:2-15:10, 85:2-5, 21:5-23:18. Not only was that construction not offered, it contradicts the specification's statement that tokens may be produced through "one or more encryption techniques …, for example, hash functions and other methodologies." EX1001, 6:58-7:5. Also, the specification explicitly acknowledges reversible encryption. EX1001, 7:34-43 ("unencrypted"). Regardless, both Evenhaim and Settimi teach hash functions for tokenization, as discussed above.

search."), [0050], [0073]; EX1015, ¶¶11-12, 14. Settimi also explains that a user can search using any terms desired. *Id.*, [0061]. Thus, Vigilytics' argument fails.

Additionally, Vigilytics treats the POSA as an automaton with no ordinary creativity. *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). At the time, there were varied interests in searching for patient data, whether for searching for disease states (by pharmaceutical companies) or for particular patients (by insurance companies). EX1014, 47:12-50:15; EX1007, [0003], [0008], [0025], [0037]. As Vigilytics' expert admits, a POSA would have understood that a database containing health records would not be limited to one type of search and that Settimi's relevant disclosure (*see* EX1006, [0030]) is "very broad." EX1014, 47:12-50:15, 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, 44-46; EX1014, 83:3-8; *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").

Second, the combination does not run contrary to Evenhaim's true preference. Evenhaim seeks to maintain a rich dataset, as compared to low-resolution datasets. EX1005, 7:46-58; EX1015, ¶15. The lower resolution datasets, according to

Evenhaim, precluded analysis of "a predefined list of consumers." *Id.*, 16:46-17:3, 3:32-41. Specifically, prior databases aggregated information into a pool of, *e.g.*, physician level or zip code level data, which prevents linkage to a particular patient. EX1005, 17:31-36 (physician level), 1:10-50 (zip code); EX1015, ¶¶13-16. Settimi's database, however, preserves individual medical records, while only tokenizing PII for those records. EX1006, [0060]-[0061], [0063]. Consequently, the combination permits the searching (using tokens) of a "predefined list" of patients—Evenhaim's goal. EX1015, ¶¶13-16. The combination simply uses a centralized database, for which Settimi identifies additional benefits. 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.

Furthermore, Vigilytics' argument that Settimi's database lacks the original raw data (due to de-identification) purportedly sought by Evenhaim is misdirection. Specifically, Evenhaim describes searches in which the patient is identified other than by his/her name. EX1005, 8:30-43 ("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[]"). Also, Evenhaim acknowledges that the "micro-level records" (*i.e.*, patient level data) that it seeks to maintain are not harmed by the removal of PII inasmuch as Evenhaim references "*identity-free* micro-data." *Id.*, 10:29-32, 12:36-52, Fig. 4 ("micro data"), 12:35-42;

EX1014, 61:17-67:2 (distinguishing micro-level data from physician level data); EX1006, [0038], [0043]. Thus, Evenhaim does not teach against the use of records that have already been stripped of PII (e.g., the patient's real name).

Notably, regarding Evenhaim's explanation that a search may use an ID rather than a name (EX1005, 8:30-43), the uncontested construction of "token," is an "identifier." Pet., 7-8. Evenhaim's aggregator's conversion of the user's query into something that the database understands, which may be an "ID or the like[]," meets this definition. EX1005, 8:30-43, 49-55; EX1025, 39:13-42:9.

D. Vigilytics' Alleged HIPAA Problem is Illusory

Vigilytics argues 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, 22-25. Specifically, the bad actor, in using a key to encrypt (*e.g.*, tokenize) a patient's PII, allegedly would save the tokens and original names in correspondence to attempt to look for the same tokens in the returned search results to determine patient identities.

This argument has nothing to do with what is claimed. In fact, the '651 Patent's design would be subject to the same type of attack inasmuch as the token generator 314 at the encryption server is not part of any closed off healthcare system (*i.e.*, source sites), as shown in Figure 3. EX1001, Fig. 3, 7:34-36, 9:46-66. When

Vigilytics' expert was asked about this problem, he explained that it would be left to a POSA to address with "known security techniques." EX1014, 25:13-28:17. He posited that one known method would be using an agreement with a trusted party. *Id.*, 52:2-53:17. Thus, the possibility of a bad actor has no bearing on the claims of the '651 Patent.

Vigilytics' expert also offered that his basis for (improperly) reading HIPAA compliance into the claims is the mere mention of the same in the specification; however, his theory would also require assuming that the applied references would also be implemented in a HIPAA compliant manner, as they also discuss HIPAA. EX1025, 86:15-87:6. Indeed, both Evenhaim and Settimi are directed to *achieving* HIPAA compliance. EX1014, 33:12-34:4; EX1005, 2:5-26; EX1003, ¶¶ 135-36. Thus, options for HIPAA compliant implementation, does not affect the application of the references.

Furthermore, as explained above, Settimi creates tokens using a hash function. EX1006, [0038], [0041]; EX1001, 6:59-7:5; EX1014, 93:13-99:18. Evenhaim also uses a hash function, which Vigilytics' expert acknowledges qualifies as a token as claimed. EX1005, 8:43-48, 12:24-34; EX1014, 79:5-20, 53:18-54:20, 37:8-38:9. The '651 Patent suggests that "hash functions or other methodologies" comply with HIPAA. EX1001, 6:59-7:5. Thus, Vigilytics' attack contradicts its own patent.

Nevertheless, out of an abundance of caution, Datavant addresses options

known to guard against hypothetical bad actors. EX1015, ¶¶17-23.

1. Escrow Agent

Regarding the concern that a party other than a HIPAA covered entity (*e.g.*, a doctor) may hold the means of tokenization (as in the ’651 Patent itself), and could misuse the same, Evenhaim offers a specific solution. Evenhaim describes tokenization at the aggregator (EX1005, 12:24-34) and that, to avoid any concern, the encryption key may be controlled (at that site) by an “escrow agent.” 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 encryption and that agreements could be used to ensure privacy. EX1014, 51:17-53:17, 29:13-30:10 (“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. Again, the very purpose of these systems is so that the patient’s identity is “not knowable.” EX1005, 13:1-20; EX1014, 25:13-28:17; 51:17-53:17, 13:33-39; EX1015, ¶¶17-23. HIPAA itself acknowledges the use of business agreements to maintain privacy. EX1021 (defining business associate), EX1020, 3; EX1016, 6.

2. Well-Known Cryptographic Methods

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 had 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, ¶¶22-23. Vigilytics' expert acknowledges such attacks have been known since the 1990s. *Id*. He also acknowledges that, since the 1990s, there have been known defenses. One defense is a "salt," in which the 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; EX1015, ¶¶22-23, 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 known mechanisms for a POSA to guard against Vigilytics' hypothetical attack, if it were a concern. *Id*.

Additionally, Vigilytics seems to criticize Datavant's expert's explicit identification of another known defense—namely, applying additional encryption before returning query results. POR, 25-27; Ex. 2001, ¶111; EX1003, ¶¶41-42; EX1015, ¶23. Specifically, Vigilytics appears to allege that Dr. Clark's testimony 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, the same is discussed in, for example, U.S. Pat. No. 7,668,820. EX1024, 2:20-51, 5:26-61; EX1015, ¶23.

3. HIPAA Rules

HIPAA provides numerous compliance options that are left to the designer to

implement. One option is the expert determination method. EX2006 (§ 164.514(b)(1)); EX1016, 12-13. This method allows for de-identification through accepted statistical and scientific methods, which leave a small risk that the information could identify an individual. *Id.* This gives a POSA latitude in determining an appropriate method of rending information sufficiently de-identified. *See* EX1016, 14, 16-18, 25-30. On this point, Vigilytics' POR confirms that a POSA "would also have familiarity with medical records and databases for storing medical records—particularly in manner that complies with privacy laws and regulations such as HIPAA." POR, 8; EX1016, 14.

HIPAA also provides a safe harbor option for de-identification that allows compliance through the removal of specific identifying information. EX2006 (§ 164.514(b)(2)); EX1016, 9-11 ("safe harbor"); EX1014, 101:12-10:2; EX1006, [0009]. Once the specified information is removed so as to, *e.g.*, provide the same to a searchable 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*. De-identification (and re-identification) in this manner can be achieved by encrypting patient identifying information with, *e.g.*, a hash function (Evenhaim's and Settimi's method). EX1016, 30-31; *see* EX1005, 14:56-67; EX1006, [0009], [0014], [0017], [0027]; EX1017, 3; *see infra* § V.

Ultimately, a POSA would have no reason to doubt that Evenhaim and Settimi

comply with HIPAA and/or could be implemented to comply with HIPAA. EX1014, 34:5-37:7, 121:22-122:9, 126:5-7.

IV. Ground 1 –Evenhaim and Murphy

A. Evenhaim Suggests Producing Tokens

For Ground 1, Vigilytics seeks to limit the encryption described in Evenhaim to general encryption for data transmission. POR, 16-19. However, Evenhaim describes different encryption for the patient list and the overall message, such that the encryption/tokenization of patient names differs from transmission encryption. EX1005, 13:33-43, 14:3-13. Further, Evenhaim states that *parts of the parameter list* may be encrypted, including through a hash. EX1005, 8:43-48, 12:24-34 (explaining that encryption can happen anywhere in the system); EX1014, 79:5-20, 53:18-54:20, 37:8-38:9. Thus, Evenhaim suggests that, separate from general transmission encryption, parts of the list (*e.g.*, 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 transmission encryption. EX1015, ¶¶27-28.

Vigilytics' expert acknowledged Evenhaim's teachings on this point and admitted that the enhanced encryption for parts of the parameter list (which he calls "super encryption") would remain *after* the transmission encryption is decrypted at

the data source. 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 meets the claimed tokenization. EX1015, ¶¶28-29.

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, 12:24-34, 8:43-48, 11:43-46 (functions can be reversed). Vigilytics' argument is that it would happen in only one place in Evenhaim—after the searching—which contradicts Evenhaim's statements. *Id*.

Also, Vigilytics' expert acknowledges that systems such as Evenhaim's employ standard formatting to make queries workable. EX1014, 57:15-6; EX1005, 8:30-56 ("a combination of a few fields that together can allow for identification"), 13:1-12, 10:37-41. 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. This disclosure on its own qualifies as tokenization under the accepted construction. Pet., 8.

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 (POR, 29-30), the use of "may" confirms Evenhaim is not so limited. EX1005, 9:45-51,

8:30-43, 13:33-43.

B. Whether Tokenization Would Benefit Evenhaim

Vigilytics argues that there would be no need to de-identify Evenhaim's patient list or query through encryption. POR, 23-29. But Evenhaim *explicitly describes encrypting both* (using higher encryption levels for the list), as discussed above. Thus, the question is simply whether it would have been obvious to perform de-identification of the parameter list based on Evenhaim's explicit disclosure of encrypting such information before 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 '651 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"

There is also no "teach[ing] away" from agglomerated data or token matching. POR, 27-28, 34, 1. As discussed above, Evenhaim merely states that low resolution data is not robust enough for some applications. EX1005, 3:32-41, 5:4-7, 1:38-50.

D. Evenhaim and Murphy Suggest Determining Minimums According to a Privacy-Preserving Rule

The POR attacks Murphy on claim element [7.g] but fails to address Petitioner's citations to (and reliance on) Evenhaim. POR, 31-34; Pet., 26-27.

Evenhaim's protocols apply a minimum number of individuals at the front end (query) and back end (search results) to safeguard patient identity. EX1005, 13:62-65, ("a predetermined minimum number of individuals … into a 'parameter list'"), 8:13-48 ("large enough list"; "transmitting the parameter list may include transmitting a sufficiently large list"), 16:5-32 ("The query engine determines whether the number of participants in each program and the % ***participants matched*** are above a level that ensures consumer individual privacy …. If not, the query engine responds with: group name 'cannot be analyzed because of privacy safeguards.'"); Pet., 26-27 (citing these sections of Evenhaim); EX1015, ¶24. Vigilytics' expert admits that Evenhaim enforces minimums at the query side and data source side. EX1025, 42:10-47:22. Thus, Vigilytics attack against Murphy alone fails.

Regardless, Murphy suggests feature [7.g]. Murphy describes checks to ensure at least a minimum number of records were identified. EX1009, 553; EX1015, ¶25. If that minimum is not met, a message is provided that says "<3." *Id.* That does not answer the query posed (*e.g.*, stating the number of hits). *See* POR, 67 ("rather than returning an absolute value"). Vigilytics' expert admitted that this minimum is applied at the data source side. EX1025, 42:10-47:22. And, contrary to Vigilytics' argument, Murphy is not limited to the nature of the query. EX1009, 555 ("acceptable methods of obfuscation will be dependent on the types of data that need

to be served back to the client application”).

Regarding the “rule that disallows same individuals to be included within a defined period of time” ([7.h]), Murphy describes tracking a user’s search history to ensure that similar query results are not permitted within a predefined time period. EX1015, ¶26. Specifically, Murphy describes tactics that force a bad actor to perform repeated searches directed to the same information in order to “create[] a detectible pattern.” EX1009, 554. If, *e.g.*, the “exact same number of patients were returned in previous queries within a specific time period,” the system blocks the user’s queries. *Id*. While the example query uses the “number” of patients, the concept is not limited to one query type, 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”). Ultimately, Evenhaim’s queries are for specific patients and Murphy’s teaching is applicable to any query, as the common goal is preventing identification of a particular patient. EX1009, 552 (“imperative that single individual could not be identified through user interface”), 553 (“the key … is to make attempts to discern individuals … recognizable”), 554; EX1025, 48:1-50:11. And Vigilytics’ expert (i) acknowledged that a POSA would understand that various types of attacks of this nature need to be guarded against and (ii) did not dispute that Murphy’s example may fall within the scope of the claims in any event. EX1025, 51:15-53:5, 61:11-62:12.

V. Ground 3: Dick, Landi and Murphy

A. The References

1. Dick

Dick describes a query for a group of individuals. EX1007, [0024]-[0025]; EX1014, 114:2-115:9; EX1015, ¶30; Pet., 57-62. While Dick recognizes HIPAA restrictions and "contemplates" "methods and processes" for de-identification, it does not mandate specific processes. EX1007, [0046]-[0047]; EX1014, 111:7-113:6; EX1015, ¶30.

2. Landi

Landi describes de-identifying patient records using an encrypted ID (a token). EX1015, ¶31. The tokens enable patient records to be located and released to third-parties without revealing patient identities. EX1008, 10:15-31, 14:26-29; EX1015, ¶31. Landi contemplates re-identification of records, but only by authorized entities. EX1008, 7:22-30, 2:5-49, 5:32-47, 8:16-63.

B. Motivation to Combine Dick, Landi and Murphy

Vigilytics alleges a lack of a motivation to combine Dick, Landi and Murphy because Dick already discloses de-identification. POR, 48-51. However, the paragraph cited by Vigilytics merely identifies the general de-identification options under HIPAA. EX1007, [0045]; EX2006 (§ 164.514). Dick is only telling a POSA the options in general terms, without endorsing a particular technical operation. EX1015, ¶32. Vigilytics also argues Dick obtains consents, obviating the need for

de-identification under HIPAA. That contradicts Dick's stated goals—namely, de-identification. EX1007, [0046].

The other paragraphs that Vigilytics cites, [0046]-[0047], do nothing more than discuss the goals and benefits of de-identifying. EX1007, [0046] (medical research), [0047] (finding study patients). Again, no specific techniques are mandated. The Dr. Clark testimony cited by Vigilytics does not change this understanding. POR, 48-51. 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: Landi's. EX1015, ¶¶32-33. As Vigilytics admits, simple de-identification is not the issue here. POR, 58 ("not directed to mere … 'de-identification.'"). A POSA would have found it obvious to select any technical method, including Landi's.

Also, de-identifying was not the only reason given for the combination. The Petition also relies upon on Landi's "central database" design as a rationale. Pet., 59-61.

Vigilytics also contends that a POSA would not use Landi because it is allegedly not HIPAA compliant. POR, 58-59. The general failure of this argument is addressed above with respect to Ground 2. Specifically, Landi explicitly states that its design presents "no HIPAA issues." 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. At base, Landi describes a tokenization method for a 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, ¶34.

Notably, while Vigilytics argues that Landi's particular encryption option "violates HIPAA[]" (POR, 51-52), this argument conflicts with the '651 Patent and the claim construction of "token," inasmuch as tokenization only requires an ID to be used (Pet., 8) and the '651 Patent calls for *any encryption method* for HIPAA compliance (EX1001, 6:34-38). Notably, while Vigilytics takes issue with Landi's use of an encryption technique that allows for decryption, the HIPAA allows for re-identification (EX2006 (§ 164.514)) and the official comments of the rule state that the re-identification provision "does not preclude" "cryptographic" options (EX1016, 30-31). *See* EX1008, 2:49-53 (discussing safeguarding of the key). Finally, Landi also explains that its encryption keys are controlled by a "trusted broker" and only disseminated to authorized entities. EX1008, 8:5-15. Thus, Vigilytics' argument is misplaced.

C. The Combination Suggests Producing Tokens for Individuals

Vigilytics asserts that there is no need for the requester's server to send tokens rather than patient names. POR, 56-57. This argument relies on a hypothetical posed to Dr. Clark and cites his testimony out of context. POR, 56-57. For the hypothetical, Dr. Clark was not analyzing any references in this ground, but instead discussing Evenhaim. EX2002, 57:16-25, 60:12-23. As discussed above, Evenhaim *explicitly discloses* performing encryption of the names before they are sent, making the argument that the same is not needed moot. In any event, the testimony has no bearing on the present combination. Also, the argument ignores that Landi's centralized database would not know patient names, inasmuch as the records are already tokenized, as Vigilytics' expert admits. EX1014, 131:1-132:4; EX1008, 7:3-38. Thus, tokenization is needed to match the language Landi's database understands.

Vigilytics also argues that Landi does not describe querying names. POR, 57-58. However, it is Dick that is relied upon for the query content. EX1008, 4:40-46, 11:23-29. A POSA applying Dick's search for patients in Landi's database would understand that the manner of finding the same would be through searches for encrypted IDs (tokens). This is not hindsight bias, it is a simple understanding that a query would speak the language used by the database. EX1014, 47:12-50:15; *see* EX1009, 556.

Additionally, the record establishes that the encryption in Landi is not restricted to only patient centers. For example, 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, 9:16-19; POR, 55. A POSA would understand that encryption/tokenization can occur where useful.

Finally, Vigilytics' argument that a POSA would not make the combination because Murphy purportedly "rejected" de-identification also fails. POR, 64, 68. Murphy recognized that de-identification may not be sufficient *alone* to protect privacy, so Murphy added obfuscation techniques. 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 search parameters were narrow enough. Murphy does not reject de-identification, but supplements it. EX1009, 552-554. Thus, a POSA would not be dissuaded from combining Murphy with Dick and Landi.

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, 59-63.

First, deficiencies in this argument are already addressed above. Second, Landi explicitly states that PII 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 teaches the usefulness of the encrypted IDs when processing and searching for data. EX1008, 8:23-55, 11:23-29 ("enable the same patient to be recognized at different collection times"), 11:52-63 ("[P]atient data is typically maintained in database tables . . . and can readily be searched.").

Regardless, the combination relies upon Dick for teaching the searching for specific patient records. Pet., 60-63; EX1003, ¶222.

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, Landi and Murphy is not "unattainable" PII. POR, 63-64. Dr. Clark merely stated that returned information in Landi may include the encrypted ID. EX1015, ¶35. That does not mean that "PII is available in the produced healthcare information." POR, 64. 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. This is consistent with the '651 Patent, which explains that its tokens are encrypted PII. EX1001, 2:8-15, 6:53-57, 7:2-5, 7:34-37. In any event, Landi accomplishes unattainability by protecting the decryption key. EX1008, 2:49-53.

Therefore, Vigilytics argument fails. EX1015, ¶35.

F. Murphy Teaches Using Minimums to Block Attacks

As explained above, Murphy checks to ensure a minimum number of records are identified or it responds "<3." *See supra* IV.D; *see also* EX1025, 51:15-53:5. That does not answer the query posed (*e.g.*, 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 for reasons addressed above.

Vigilytics also improperly isolates Murphy from its combination with Dick and Landi to argue that Murphy is only concerned with returning a number of patients, as opposed to patient records. Though Murphy may, in its example, identify the number of records, 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, ¶¶36-38. That concept is applicable regardless of the nature of the query, as discussed above. *See* 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"). And, in any event, the claims merely require the return

of "medical information that characterizes a group," which would be met by providing the number of patients with a specific ailment. EX1025, 61:11-62:12.

G. 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. EX1009, 552 ("An attack on the system would occur by someone entering criteria into the query tool that would result in only one matching person."), 553 ("attempts to discern individuals"). EX1015, ¶37. A POSA would understand that the precise point of the blocking is a design choice. EX1015, ¶39. 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.

H. Vigilytics Misconstrues Murphy

Vigilytics argues that Murphy's method is not conditioned on the number of individuals from the group indicated in the request because Murphy says its method "does not limit the logic of the query." POR, 67-68; EX1009, 556. As the full quote shows, Murphy is simply explaining that users are not limited in the parameters they can enter into the request (*e.g.*, "data elements or values that can be used in the

query"). EX1009, 556. Murphy goes on to state that its method allows "general research queries." *Id.* A POSA would understand that Murphy allows for typical queries to be asked but will only answer the request if a sufficient number of individuals are in the result. EX1003, ¶¶227-31. It would have been obvious for a POSA to implement this prior to sending the request for medical information for the reasons discussed above. *Supra* §§V.F-G.

VI. Conclusion

For these reasons, the Challenged Claims are unpatentable.

DATED: February 27, 2025

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 5,419 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: February 27, 2027

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:

IPR25412-0022IP1@fr.com
PTABInbound@fr.com
axf-ptab@fr.com
barclay@fr.com
nstephens@fr.com

DATED: February 27, 2025

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