

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DATAVANT, INC.,
Petitioner,

v.

VIGILYTICS LLC,
Patent Owner.

Case IPR2024-00226
Patent 9,118,641 B2

PATENT OWNER'S SUR-REPLY

TABLE OF CONTENTS

I. INTRODUCTION 1

II. THE CHALLENGED CLAIMS ARE PATENTABLE OVER GROUNDS
1-4 2

A. Ground 1 – Evenhaim.....2

1. Evenhaim Explicitly Teaches Away From Searching De-
Identified Datasets as Datavant Proposed in the Petition.2

2. Datavant Errs in Mischaracterizing Evenhaim’s Goal of
Searching Original Patient Data as a Mere “Preference”
for “Robust” or Patient-Specific Data, Even if the Data
has Been De-identified 4

3. Evenhaim Never Encrypts PII to Create Tokens for Individuals
in the Group Characterized in a Request for Healthcare
Information 7

B. Ground 2 – Evenhaim in view of Settimi.....10

1. Evenhaim Teaches Away from Searching a De-identified or
Limited Data Set Warehouse Like Settimi’s, and
Datavant’s Reliance on Settimi’s Limited Data Sets Fails
to Address Evenhaim’s Concern or Meet the Claim
Requirement for “De-Identified” Data 10

2. Settimi Does Not Disclose Use of Encoded Patient Identifiers
(EPIDs) for Searching a Data Warehouse, and Datavant’s
Proposed Use of EPIDs in the Evenhaim-Settimi
Combination is Unsupported, Infeasible, and Not
Compliant with HIPAA 13

3. Datavant’s New Reply Theories Fail to Remedy the HIPAA
Violations That Predictably Result from the Evenhaim-
Settimi Combination.....17

a. HIPAA’s Safe Harbor Protections are Non-Availing 17

b.	HIPAA’s Business Associate Exception is Non-Availing	18
c.	The Reply’s New Encryption Theories are Non-Availing	20
C.	Ground 3 – Dick in view of Landi	21
1.	Landi’s Encrypted IDs, as Applied in the Dick-Landi Combination and Included in the “Produced Healthcare Information,” are not “Absent Personally Identifiable Information” as Required by Independent Claims 1, 7, and 14.....	21
2.	Datavant Fails to Show that Landi’s Encrypted IDs are HIPAA Compliant or that a POSITA Would Have Integrated Encrypted IDs in Dick that Violate HIPAA	22
3.	The Reply Continues to Rely on Impermissible Hindsight in Arguing that it Would Have Been Obvious to Transform Dick’s Requester’s Server into an Encryption Server that Produces Tokens for Individuals Identified in the Request	26
D.	Ground 4 – Dick in view of Landi and Murphy	27
III.	CONCLUSION.....	27

EXHIBIT LIST

Exhibit No.	Description
2001	Expert Declaration of Aviel D. Rubin, Ph.D.
2002	Transcript of Deposition of Paul C. Clark, September 26, 2024
2003	Summary of HIPAA Privacy Rules (https://www.hhs.gov/sites/default/files/privacysummary.pdf)
2004	Summary of the HIPAA Security Rule (https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html)
2005	HIPAA History (https://www.hipaajournal.com/hipaa-history/)
2006	45 C.F.R. §164.514 (Other requirements relating to uses and disclosures of protected health information)
2007	45 C.F.R. §75.2 (Definitions)
2008	Transcript of Deposition of Paul C. Clark, January 16, 2025

I. INTRODUCTION

The Reply fails to show that any claim of the '641 Patent is unpatentable, and Datavant's arguments only underscore that none of asserted prior art sought to address an equivalent problem as that addressed by the '641 Patent, let alone provided an equivalent solution.

The inventors of the primary references applied in this IPR—i.e., Asaf Evenhaim and Richard Dick—had both attempted to commercialize systems described in their patents before Mr. Andrew Paris, founder and CEO of Vigilytics, had even conceived of the technology in the '641 Patent. But neither Evenhaim's nor Dick's systems were designed to analyze de-identified healthcare data in a system that would allow an insurer to rate the cost/risk of insuring small to mid-sized groups of known individuals while complying with HIPAA, as Mr. Paris sought to do. Indeed, Evenhaim and Dick addressed other problems (e.g., health program analysis and authorized medical record retrieval).

Mr. Paris nonetheless solved the group rating problem using de-identified data with the '641 Patent, and the resulting Vigilytics' GRx platform has enjoyed resounding commercial success, producing more than \$500 million and creating more than 1.4 million reports for groups comprised of more than 62 million people in total since inception. Such success would not have been realized if Evenhaim, Dick, or the other prior art had already provided a solution this

problem. None did. And significantly, because the prior art was directed to different problems/solutions than the '641 Patent, the relied-upon prior art disclosures fail to align with the '641 Patent claims, leaving Datavant to distort/misapply their teachings and propose non-obvious prior art combinations that do not even comply with basic regulatory requirements like those defined in HIPAA.

For these and other reasons described below and in the POR, Vigilytics respectfully submits that the patentability of all claims should be confirmed.

II. THE CHALLENGED CLAIMS ARE PATENTABLE OVER GROUNDS 1-4

A. Ground 1 – Evenhaim

1. Evenhaim Explicitly Teaches Away From Searching De-Identified Datasets as Datavant Proposed in the Petition

The Petition maps Evenhaim in a manner directly at odds with Evenhaim's goal of analyzing original patient data *before de-identification*, and thus fails to disclose or render obvious multiple claim limitations, as discussed in the POR. POR, 15-34. The Reply contends that “[t]here is [] no ‘teach[ing] away’ from agglomerated data or token matching” in Evenhaim, but this misses the point. The problem is a failure by Petitioner to address the salient issue – Evenhaim teaches

away from searching data that has been *de-identified*.¹ Indeed, the Petition relies on a directly opposed and inaccurate view of Evenhaim. *See, e.g.*, Pet., 10, 13-14, 18-19 (searching HIPAA-compliant “de-identified” patient data). Generating de-identified patient data requires removing a range of personally identifying information (PII) that could be used to identify a patient, and de-identified data is inherently less granular/robust than the original patient data. EX2006, 2-3. The standard de-identification method required by HIPAA (i.e., the so-called “Safe Harbor” method), for example, requires removal of at least **18** different types of identifiers for patient data to be validly “de-identified” before disclosure. EX2006, 1-2; 45 C.F.R. § 164.514(b)(2); EX2008, 20:8-20:23. HIPAA’s alternate “expert determination” de-identification method is similarly rigorous and requires removal of PII to the extent that the patient’s identity cannot reasonably be discerned from the de-identified data. 45 C.F.R. § 164.514(b)(1).

The Reply fails to acknowledge that the Petition’s reliance on searching *de-identified* data is problematic, despite express disparagement by Evenhaim of searching de-identified data sets, and particularly HIPAA-compliant de-identified

¹ Claims 1 and 7 require matching tokens “in a set of *de-identified* healthcare data,” as required by claims 1 and 7. Datavant cannot prevail by relying on searches of other forms of data that may not be fully de-identified.

data; Evenhaim evens characterizes de-identified data as “useless.” EX1005, 4:42-45 (“HIPAA provides substantial limitation on [PHI] and existing de-identification method may render the information *useless for the purpose of measuring the impact of health programs.*”); *see also id.*, 16:63-17:3 (lamenting that “[o]ne cannot query or analyze parameters that are no longer in the lower resolution dataset”), 7:46-52 (“precludes external researchers from benefiting from the *richness of the ‘source-entity’ data*”), 6:15-17 (“invention allow[s] analysis of ‘source-entity’ *raw data* at is [sic] *original*, most detailed form”), 16:49-50, 16:64-17:3. Evenhaim openly and consistently criticizes searching/analyzing de-identified data throughout its disclosure, as Evenhaim discourages POSITAs from applying its process to de-identified data searching, as proposed in the Petition. *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1327 (Fed. Cir. 2009) (“A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant.”).

2. Datavant Errs in Mischaracterizing Evenhaim’s Goal of Searching Original Patient Data as a Mere “Preference” for “Robust” or Patient-Specific Data, Even if the Data has Been De-identified

The Reply frames Evenhaim as expressing a mere “*preference* for ... searching robust micro-level data” in which “the level of granularity” of data

searched “would be *up to the designer.*” Reply, 3, 7. But these arguments only reinforce Datavant’s fundamentally mistaken understanding of Evenhaim’s objectives.² Searching original patient medical records at their *highest resolution* was not a matter of mere design choice for Evenhaim; it was instead the animating principle underlying the entire architecture and distributed search methodology of Evenhaim’s system. EX2001, ¶¶119-121, 143-144. Indeed, Evenhaim’s goal of searching the highest resolution, original patient data—*before de-identification*—is the essential reason that Evenhaim burdens healthcare providers (i.e., “data source entities”) with carrying out searches at their local systems rather than outsourcing the search to the aggregator or other centralized database where the patient data would need to be de-identified. EX1005, 6:15-25, 9:29-67, 17:43-52, FIGS. 4-4A. The providers are the only entities under HIPAA that can maintain,

² Datavant also overlooks that “even if [the prior art] is not found to teach away, its statements regarding preferences are relevant to a finding regarding whether a skilled artisan would be motivated” to implement de-identified data searching in Evenhaim. *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1069 (Fed. Cir. 2018). Evenhaim’s repeated admonition of de-identified data searching is contrary to Datavant’s interpretation of Evenhaim and its proposed motivations to implement de-identified data searching in Evenhaim.

access, and search the original patient data records at their highest resolution.

EX2001, ¶¶119-121, 143-144.

The Reply misses these points entirely, disregarding overwhelming evidence that Evenhaim would not have desired searching on de-identified datasets as proposed in the Petition. Indeed, the Petition’s Evenhaim grounds are noticeably premised on the exact type of search that Evenhaim sought to avoid:

Approach Disparaged by Evenhaim:

By contrast, an example of “classic” model of health analytics calls for aggregation of de-identified patient-level or physician-level data which allow the central analysis model only (see FIGS. 1 & 2). The common method used by existing healthcare analytics companies (such as IMS, NDCHealth and Verispan) is based on the following steps: (A) De-identify & Aggregate—patient data is de-identified (some data is removed or grouped together) and data is reported typically at the physician level. In some cases the dataset includes longitudinal de-identified patient-level data (such as Verispan and Dendrite) (B) Collect from various sources—data is collected from multiple healthcare organizations into a data warehouse (C) Analyze—syndicated data reports and custom studies are produced.

Evenhaim’s “Crossix” Method:

The instant Crossix “method” is based on an opposite sequence: (A) Analyze—the healthcare organization (such as health plan) runs an analysis software that receive as an input the required analysis and aggregation level as well as possibly a list of identifiable patients or physicians for which analysis is requested. This analysis is performed on the original, most complete data set; (B) De-identify & Aggregate—Once name matching and analysis is complete data is aggregated and, if needed, de-identified; (C) and Collect from various sources—Analysis responses from multiple organization are composed to deliver the analyses requested.

EX1005, 17:28-52; *see also id.*, 4:42-45 (“de-identification method may render the information *useless*”), 6:15-17 (“invention allow[s] analysis of ‘source-entity’ *raw data* at is [sic] *original*, most detailed form”), 16:49-50 (“high-resolution *raw data* that includes the *maximum* amount of information”), 16:64-17:3 (“existing” models are not satisfactory because “[o]ne cannot query or analyze parameters that are no longer in the lower resolution dataset”).

The Reply misleads by suggesting that Evenhaim’s data sets “are not harmed by the removal of PII inasmuch as Evenhaim acknowledges the option of ‘*identity-free* micro-data,” and that “agglomerated data can be as robust as the

designer intends.” Reply, 8, 17; *see also id.*, 3. Whatever truth those statements may have with respect to data sets returned *after* a search, they are defied by the above and other statements from Everhaim regarding source-entity data sets and the importance of searching before converting to a *lower resolution dataset* to avoid rendering the information *useless*. For example, the Reply cites col. 10:29-41 of Evenhaim on several occasions, but this portion of Evenhaim refers to the operation of “agglomerating *the extract*,” i.e., an operation performed *by the data aggregator* on a search *extract* received from the data source entities *after* a search on the original patient data has generated data subject to the extract. EX1005, 10:29-41. Datavant’s additional citations are similarly unavailing. *See, e.g.*, EX1005, 12:36-67 (describing search results that are “aggregate[ed]” *after* the data set is searched but before an aggregated result is returned); *see also id.*, 6:64-7:26 (describing operations for “agglomerating 340 the extract” and “crunching together” data items returned from the source entities *after the search*), FIG. 3; *infra*, Section II.A.2.

3. Evenhaim Never Encrypts PII to Create Tokens for Individuals in the Group Characterized in a Request for Healthcare Information

Datavant again fails to show that the encryption performed by Evenhaim’s data aggregator produces tokens for individuals in the request as claimed. With reference to a single statement in Evenhaim that “all or part of the parameter list”

may be encrypted, the Reply contends that “separate from general transmission encryption, ... patient names, may be separately encrypted” to produce tokens for the individuals identified in the request. Reply, 14 (citing EX1005, 8:43-48). But Datavant’s argument is not consistent with the context in which the statement it relies upon is made. Evenhaim’s reference to encrypting “all or part of the parameter list” comes at the end of a paragraph describing how the query or parameter list can include one or more different *types* of parameters used to define a target patient population, such as “geography, age or other attributes,” or by “name or ID or the likes.” EX1005, 8:30-48. Dr. Rubin explained that, at best, a POSITA would have understood this vague statement to mean that “certain *types* of fields aren’t encrypted and others are,” consistent with the full context of Evenhaim’s disclosure. EX1014, 77:21-79:4. Dr. Rubin rejected any notion that a POSITA would understand this disclosure to mean that “certain names are encrypted and others aren’t.” *Id.*, 78:19-79:4. It also makes no sense why Evenhaim would leave some patient names unencrypted, and Datavant has offered no explanation why different encryption standards would be applied to different patients. For example, Datavant does not address how the data source entities would use both encrypted and unencrypted patient names for searching a de-identified data set, which may not even be possible. Vigilytics’s POR, by contrast, cited Evenhaim’s repeated explanations that the entire “patient list” is

encrypted as opposed to individual patient names, and that the data source entities decrypt the list to locate records by matching names, not tokens. POR, 16-23; EX1005, 13:33-43, 14:3-13, FIGS. 4-5.

Datavant's attempt to inject tokenization in Evenhaim based on "super-encryption" also fails. Not only is the "super-encryption" theory improper since it was never presented in the Petition and never discussed in Evenhaim, but the theory is also non-sensical because the purpose of super-encryption is to hide certain information from the recipient of a message that the recipient cannot decrypt. EX1014, 77:3-11. But HIPAA does not require concealing patient names or other PII from the data source entities as Datavant now proposes. EX1014, 77:2-11; EX2001, ¶¶ 110, 116, 156. The data source entities already know the identities of the patients and their protected health information, which explains why Evenhaim never proposed concealing the patient list from the source entities in the first place. EX1005, 9:45-51, 12:53-61, FIGS. 4-5.

Finally, the Reply's new theories that other parameters in Evenhaim's query, such as the patient ID, could provide the claimed "token" fail at the outset. Reply, 16. Datavant not only never mapped these alternative parameters to "tokens" in the Petition, but these parameters are also not "similarly encrypted" to produce corresponding tokens between the encryption server and data server as required by the claims. EX1001, 10:43-45, 11:24-26.

B. Ground 2 – Evenhaim in view of Settimi

1. Evenhaim Teaches Away from Searching a De-identified or Limited Data Set Warehouse Like Settimi’s, and Datavant’s Reliance on Settimi’s Limited Data Sets Fails to Address Evenhaim’s Concern or Meet the Claim Requirement for “De-Identified” Data

Settimi fails to remedy any of the deficiencies of Evenhaim alone. On the contrary, based on the petition’s formulation of the Evenhaim-Settimi combination, it inherits problems exposed in Ground 1, starting with the fact that Evenhaim specifically teaches away from searching de-identified patient data. *Supra*, §II.A.1-2; POR, 27, 39-40; EX2001, ¶¶119-121, 143-144. In the combination, Datavant contends it would have been obvious to integrate Settimi’s centralized database in Evenhaim’s system such that Evenhaim’s data aggregator would query Settimi’s database instead of the original data source entities. Pet., 34-37. But Settimi’s database, as described in the Petition, stores data that has been *de-identified* or otherwise limited in information content and would require that Evenhaim’s search be performed on such lower resolution data in lieu of the original patient records. Pet., 34 (“keeping the centralized records HIPAA compliant”), 36 (“records are stripped of PII before being sent to the central repository”), 37. This runs directly afoul of Evenhaim’s instruction to search original, high resolution datasets, and would preclude Evenhaim from achieving the quality of data analysis that Evenhaim indicates is needed for its purposes.

Supra, §II.A.1-2; POR, 26-28; EX2001, ¶¶119-121, 143-144.

Datavant attempts to distinguish Settimi’s database from other “low-resolution databases,” based on Settimi’s statement that its database “retain[s] clinically useful information about the patient.” Reply, 4 (citing EX1006, [0038], [0040]). But with this statement, Datavant fails to regard that de-identified data sets can still retain clinical information or that Evenhaim’s concern with de-identified data sets would not have been cured by whatever clinical information remained in Settimi’s database. *Supra*, §II.A.1-2. This is evident because Settimi clarifies that its data is de-identified according to the *same* methods prescribed by HIPAA that Evenhaim specifically characterized as being “useless” for its purposes. EX1005, 4:42-45; EX1006, [0027] (Settimi explaining that “this document refer[s] to ... fully de-identified data as defined by HIPAA”), [0039] (“create de-identified data that would be classified under the HIPAA definitions as fully de-identified”); EX2008, 20:8-20:23. Settimi discloses no other de-identification techniques beyond those permitted by HIPAA, which makes sense because the data otherwise could not be disclosed by the PCPs to the central warehouse.

Settimi’s alternate embodiment in which the central database stores “limited data sets” is also deficient since it (i) still does not fulfill Evenhaim’s goal of searching on the original, highest resolution data and (ii) does not meet the

claimed requirement for use of “de-identified” healthcare data. Reply, 4 (citing EX1006, [0040]). Limited data sets are distinguished in HIPAA from de-identified data, and consistent this distinction, Settimi explains that “[a] limited data set is *protected health information* for research, public health and health care operations that excludes direct identifiers ... but in which *other identifying information may remain*” EX1006, [0027]; EX2006, 3-4 (*compare* 45 C.F.R. § 164.514(b) (provisions for fully de-identified data that no longer qualifies as PHI and can be freely disclosed to third parties) *with* § 164.514(e) (provisions for limited data sets that retain identifiers and remain PHI but can be disclosed for limited purposes)). Although Settimi uses the terms “de-identified patient information” and “de-identified patient data” as shorthand to simplify its description of embodiments encompassing either fully de-identified data or limited data sets (*see* EX1006, [0027])), the fact that a limited data set leaves identifying information in the data, with no determination that the patient’s identity could not be obtained from the data, is fatal because it fails to meet the claim requirements for operating on a “set of *de-identified* healthcare data.” Datavant has not established, nor attempted to establish, that a limited data set constitutes “de-identified” healthcare data in the ’641 Patent, although it is clear that such an understanding is inconsistent with the specification. *See, e.g.*, EX1001, 3:43-47 (explaining that de-identified data involves “*removing all*

personally identifiable information 118 or otherwise transforming the PHI 130 so that *it cannot be associated with a particular person*”—consistent with HIPAA’s safe harbor and expert determination methods of §165.514(b), distinguished from limited data sets). Datavant notably submitted no evidence from Dr. Clark or otherwise addressing the meaning or implications of using limited data sets, and at his deposition, Dr. Clark revealed his lack of expertise through testimony that was facially contradicted by the plain language of the HIPAA rules on limited data sets. *Compare* EX2008, 14:14-17, 17:5-11, 21:5-15, 22:7-11, 22:21-24:3, 24:24-25:21, 25:22-26:15 *with* EX2006, §164.514(b)-(e).

2. Settimi Does Not Disclose Use of Encoded Patient Identifiers (EPIDs) for Searching a Data Warehouse, and Datavant’s Proposed Use of EPIDs in the Evenhaim-Settimi Combination is Unsupported, Infeasible, and Not Compliant with HIPAA

Beyond the problems with modifying Evenhaim to search de-identified or limited data sets as discussed above, Datavant’s proposed integration of Settimi’s encoded patient identifiers (EPIDs) in Evenhaim for searching the central database suffers from additional problems that are indicative of further impermissible hindsight undercutting the Petition’s obviousness theories. Pet., 40-43; Reply, 5.³

³ Additionally, because Settimi’s EPIDs are re-identification codes that have not been irreversibly de-identified, they fail to render “the identity of the individuals

First, contrary to assertions in the Reply, the use of EPIDs for searching a centralized database is entirely unsupported by Settimi. As explained in the POR, Settimi describes methods for searching the central warehouse by specifying patient characteristics or clinical diagnoses for a target population from which a cohort of patients could be identified for a clinical trial, for example. EX1006, [0027]-[0028], [0036]-[0038], FIGS. 2-3; POR, 37-39. Settimi never contemplates searching the central warehouse by EPIDs, however. *Id.*

The Reply contends that Settimi at paragraph 47 discloses a relevant EPID-based search, but this is not the case. Reply, 4-5. Paragraph 47 only describes the ability of a user to enter an EPID *in the PCP's local electronic medical records (EMR) system*, but not to search the central warehouse. EX1006, [0047] (“A user may search for one or more patient records *within EMR* ... The user may search by the EPID[] The corresponding patient chart may be retrieved and displayed.”), FIG. 2 (showing EMRs within PCPs 106), [0049] (“Re-identification may occur *at the local system level* ...”); EX2008, 39:23-40:2. The Reply’s additional citations to paragraphs 50, 51, 71, and 73 likewise never describe any

in the group [] unattainable,” as required by independent claims 1, 7, and 14.

EX1006, [0041]-[0043], [0044]; EX2008, 35:13-18, 37:20-23; POR, 39-40; *cf.*, EX1001, 3:43-46, 5:65-67.

ability to search the central warehouse using EPIDs. *See* EX1006, [0050]-[0051], [0071], [0073].

Second, Evenhaim’s data aggregator would not be able to produce EPIDs to query Settimi’s central database because EPIDs can only be generated by an entity that possesses confidential information known only to the PCPs. Settimi explains that only the PCP produces an EPID by encrypting a patient identifier (PID) with a “password string” that “is *known only to the PCP*” and that is also “required in order to decode the EPID [] into a PID [].” EX1006, [0041]; EX2008, 32:9-33:8, 33:18-34:2. The PID is likewise a unique numeric key *assigned by the PCP* “to uniquely identify an individual patient” in the PCP’s EMR. *Id.*, [0038]. The data aggregator in the Evenhaim-Settimi combination would be incapable of producing an EPID for the individuals identified in a request because the aggregator would have no access to either the PID or the password necessary to produce the PID.⁴

⁴ Paragraph 30 of Settimi also does not suggest a capability for EPID-based searching as Datavant argues. *See* Reply, 3, 5. None of the entities identified in paragraph 30 would have access to the PCPs’ confidential PIDs and passwords as needed to create an EPID. Paragraph 30 instead suggests that the additional companies could search by conventional parameters “to create a cohort report.” EX1006, [0030].

EX2006, 2-3 (45 C.F.R. § 164.514(c)(2)); POR, 35-36, 51-52; EX2001, ¶¶138-144, 195-198.

Third, searching by EPIDs would be impractical due to variation in the EPIDs assigned to each patient by different PCPs. Because the PCP is generated based on a PCP-specific patient identifier (PID) and a PCP-specific password string, the patient's data records in the warehouse would be associated with different EPIDs depending on where the PCP originated. EX1006, [0029], [0038], [0041], FIG. 3. Consequently, a search of the warehouse by a particular EPID for a patient would fail to surface all of the patient's records from different contrary to Evenhaim's goal of comprehensively analyzing patient data from multiple sources. EX1005, 6:20-25, 10:6-11, FIGS. 4-5; EX1006, [0041].

Fourth, although Datavant posits that a POSITA would have combined Evenhaim with Settimi to "reduc[e] the risk of a HIPAA violation," Datavant fails to show that Settimi's EPIDs are in fact HIPAA compliant. Pet., 37. The record evidence suggests they are not. HIPAA requires that any "code" used for re-identification of a patient not be "derived from or related to information about the individual" and further forbids disclosure of re-identification codes to third parties. EX2006, 2 (45 C.F.R. §164.514(c)). Yet, it is undisputed that the EPIDs disclosed in Settimi are re-identification codes derived from a patient identifier (PID) and disclosed to third parties (e.g., a central warehouse). EX1006, [0004],

[0041]-[0045], [0049], FIG. 2; EX2008, 37:10-15.

On similar facts involving Landi's re-identification code (encrypted ID) in Grounds 2-3, which is also generated from PII and disclosed to third parties, Datavant's own witness, Dr. Clark, conceded that such a code violates the straightforward provisions of 45 C.F.R. § 164.514(c). EX2008, 71:6-13, . Dr. Clark's logic is equally applicable to Settimi's EPIDs and shows that Settimi's EPIDs as applied in the Evenhaim-Settimi combination also are not HIPAA compliant. The record shows that a POSITA would not have integrated features in Evenhaim that fail to comply with HIPAA regulations. Pet., 25 ("purpose of Evenhaim is ... to comply with HIPAA"). At minimum, the combination does not produce healthcare information in conformity with HIPAA as required by claims 2, 8, and 15.

3. Datavant's New Reply Theories Fail to Remedy the HIPAA Violations That Predictably Result from the Evenhaim-Settimi Combination

a. HIPAA's Safe Harbor Protections are Non-Availing

Datavant contends there would be no HIPAA violation in the Evenhaim-Settimi combination because its system would only search and disclose patient data that has been fully de-identified in accordance with HIPAA's "safe harbor" provisions. Reply, 9-11 (citing 45 C.F.R. § 164.514(b)(2)). Not so. As discussed, de-identification according to the safe harbor method is a maximal

approach to de-identification, requiring removal of a wide range of identifiers that results in significant information loss in the data that would be searched. *See* 45 C.F.R. § 164.514(b)(2), EX1005, 2:25-57; *supra*, §II.A.1. As has been discussed, this is the opposite of what Evenhaim sought to achieve. EX1005, 4:42-45

Datavant’s reliance on the safe harbor underscores that a POSITA would not have been led to combine Evenhaim and Settimi as proposed in Ground 2. *Supra*, §II.A.1.

b. HIPAA’s Business Associate Exception is Non-Availing

Datavant suggests in the Reply that various entities in the Evenhaim-Settimi combination that operate the data aggregator, central warehouse, data source entities (e.g., PCPs), and/or data consumer entities could simply establish “business associate” relationships to obviate HIPAA violations that would otherwise result.⁵ Reply, 11-12, POR, 22-26, 36-40; *see also* EX2003, 5; EX2021, 1-2; EX1020, 3. This argument fails for multiple reasons.

As the outset, the business associate argument is a new theory that

⁵ To the extent Datavant invokes business associates with respect to other grounds, the theory is improper and fails to demonstrate obviousness for substantially the same reasons as addressed here for Ground 2.

contradicts, and indeed fundamentally alters, the theories originally advanced in the Petition, which were specifically framed around de-identifying data for the express purpose of complying with the HIPAA Privacy Rule under 45 C.F.R. §164.514. *See, e.g.,* Pet., 6-7, 14, 34, 37, 43. The tokenization and de-identification techniques relied upon in the Petition are only necessary under HIPAA when there is **no** business associate agreement (since PHI could otherwise be shared freely), and noticeably, the Petition never once mentions business associates. EX2008, 43:11-14, 46:7-17.

The argument also fails on substance. No evidence/explanation exists in the record as to why it would be necessary or obvious to implement de-identification and tokens for sharing data between entities under a business associate agreement when the very purpose of a business associate agreement is to allow for the sharing of PHI that has **not** been de-identified. EX2003, 5; EX2021, 1-2; EX1020, 3. But if the Evenhaim-Settimi system did not search de-identified data or use tokens, the system could not read on limitations of the '641 claims requiring such features. EX2008, 43:11-14, 46:7-17.

Datavant also overlooks that “[c]overed entities may disclose protected health information to an entity in its role as a business associate ***only to help the covered entity*** carry out its health care functions – ***not for the business associate’s***

independent use or purposes.”⁶ Neither Evenhaim’s Crossix system (e.g., the data aggregator) nor Settimi’s central warehouse receive data that originated from the data source entities/PCPs (covered entities) for the purpose of aiding the data source entities/PCPs in carrying out their healthcare functions, as would be required under a valid business associate agreement. Evenhaim instead explains, for example, that the aggregator functions for its own independent commercial purpose including “assist[ing] ... marketing managers from pharmaceutical manufacturers or other health promotion managers” to aggregate de-identified patient data and measure the impact of a health program. EX1005, 15:3-8. Dr. Clark was likewise unable to offer any further clarity on the proposed use of business associate agreements in the combination at his deposition. EX2008, 52:10-53:1, 54:14-57:7, 53:6-54:14.

c. The Reply’s New Encryption Theories are Non-Availing

Datavant contends that the risk of unauthorized parties, such as the entity that operates Evenhaim’s aggregator, being able to identify patients by correlating the PII they possess for producing request tokens with the tokens in the de-

⁶ <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>

identified records returned from the warehouse (or data source entities) could be mitigated through use of “security measures [that have] long been known in the field.” Reply, 12-14; *see also* POR, 25-26. None of these security measures are described in the Petition’s prior art, however, and tellingly, the Reply cites all new references for these features, which again, were never mentioned in the Petition.

Id. The Reply also does not explain how or whether a POSITA would have implemented any of the newly mentioned encryption techniques in the prior art systems in a manner that would address all limitations of the Challenged Claims, or if such implementations would have been obvious. Even so, Datavant’s arguments in this regard are ultimately immaterial because they do not render Settimi’s EPIDs HIPAA compliant or address any other of the various problems with the combination that have been detailed both here and in the POR.

C. Ground 3 – Dick in view of Landi

1. Landi’s Encrypted IDs, as Applied in the Dick-Landi Combination and Included in the “Produced Healthcare Information,” are not “Absent Personally Identifiable Information” as Required by Independent Claims 1, 7, and 14

Datavant does not deny that Landi’s encrypted ID in the produced healthcare information includes personally identifiable information (PII), even though the claims require an “absen[ce]” of PII. Reply, 23-24; *see also* POR, 62-63. Datavant instead contends that the encrypted ID meets the claims because “a

returned record would be associated with only the encrypted ID, with no ability to decrypt it.” Reply, 24. But Datavant’s argument conflates the “*absence*” of PII as claimed with the *accessibility* of PII (not claimed). Under Datavant’s logic, the money in a safe stocked with cash would be “absent” from the safe just because a key is needed to unlock it. Just as cash is plainly present (not absent) in the safe, PII is also present (not absent) in Landi’s encrypted ID, and Datavant does not contend otherwise. EX1008, 2:46-48, 5:18-19, 11:6-29, FIG. 3. Nor could Datavant contend otherwise, as this distinction implicates a key aspect of the ’641 Patent’s disclosure, which explains how produced healthcare information (e.g., report 212) does not simply limit access to PII data found therein; it instead generates a report based on irreversibly deidentified information, with no PII, consistent with the “absence” of PII required by the plain language of elements [1.h], [7.h], and [14.h]. *See, e.g.*, EX1001, 6:8-15 (“report generator 328 [] process[es] the requested de-identified data 208 in a way that leaves it irreversibly de-identified”), 4:52-54, 7:11-15.

2. Datavant Fails to Show that Landi’s Encrypted IDs are HIPAA Compliant or that a POSITA Would Have Integrated Encrypted IDs in Dick that Violate HIPAA

Datavant attempts to dismiss the HIPAA violations that would result from the Dick-Landi combination as discussed in the POR by referring to Landi’s statement that its design presents “no HIPAA issues.” Reply, 20; *see also* POR,

51-52; EX2001, ¶¶146-152, 170-198. Apart from accepting Landi's representation of HIPAA compliance, however, the Reply does not substantively engage with Vigilytics' observation that Landi's encrypted ID fails to comply with HIPAA regulations governing the derivation, use, and disclosure of re-identification codes under 45 C.F.R. § 164.514(c). POR, 51-53.

But relying on the representations of a patent author about its own compliance is not how a POSITA would approach HIPAA compliance. EX2008, 68:23-69:2. Indeed, this record reveals that Landi cannot be trusted in suggesting that its encrypted IDs comply with HIPAA. To this point, it is undisputed that Landi's encrypted ID is a re-identification code that is derived from the patient's PII and that is not irreversibly deidentified; more, as in the combination with Dick, Landi discloses the encrypted ID without authorization. EX2008, 63:24-64:9-65:6. The encrypted ID thus fails to meet both the derivation and security prongs of the re-identification code provisions of HIPAA § 164.514(c). POR, 51-52; EX2001, ¶¶170-173, 195-198.

In attempting to establish a basis for contending that Landi is indeed HIPAA compliant, the Reply cited to the original declaration from Dr. Clark. But during his intervening deposition, Dr. Clark conceded that he had merely accepted and repeated Landi's representation without performing any independent compliance analysis:

Q. Did you check whether the author of Landi is a HIPAA expert before stating in your declaration that a POSA would have no reason to doubt Landi's statement regarding HIPAA compliance?

A. Of course not. I didn't -- I didn't pull their biography, Counselor.

Q. Well, did you check whether Landi's encrypted IDs comply with the provisions in subsection (c) of the HIPAA Privacy Rule?

A. I did not because the statement that I made also allowed for associate agreements, so I had no reason to doubt that the system could be implemented in a HIPAA-compliant manner.

EX2008, 69:3-15; *generally id.*, 66:14-71:13.

Here, rather than identify independent compliance analysis from within his declaration, Dr. Clark attempts to explain away his failure to offer the same. For his excuse, Dr. Clark suggests that his statement allowed for implementation through associate agreements. That is, Dr. Clark contended that his failure to review the HIPAA regulations on re-identification codes was a consequence of his assumption that any HIPAA issues would be resolved by a business associate agreement. But business associates were never mentioned in Dr. Clark's first declaration (or the Petition). And, regardless, the business associate exception also fails for substantially the reasons described above in Ground 2. *Supra*, § II.B.3.b. Still, pressed to review the relevant regulations under § 154.514(c), Dr. Clark ultimately revised his opinion and acknowledged that Landi's encrypted ID

does indeed violate HIPAA:

Q. Let's consider a scenario where there is no business associate agreement in place. If we generated Landi's encrypted ID in this manner, would it violate the re-identification provision that we just reviewed from the HIPAA Privacy Rule?

A. Strictly speaking, if you did not have an associate agreement, then you would not be compliant with the derivation requirement.

EX2008, 71:6-13.

Dr. Clark's admission is striking considering that HIPAA compliance was of paramount importance to a POSITA. *See, e.g.*, EX2008, 61:8-23; EX1003, ¶¶34-36, 201, 203, 214-215, EX2001, ¶¶64, 72, 161-162. And this importance is apparent from even Dick, the primary reference in Ground 3, whose "purpose" is described in the Petition as "compliance with HIPAA." Pet., 53. Even Dr. Clark emphasized Dick's goal of HIPAA compliance and agreed that "it wouldn't make sense" to modify Dick to implement features that were not HIPAA compliant. EX2008, 62:9-18; EX1003, ¶201 ("Dick describes or suggests de-identification for complying with HIPAA."), ¶¶202-203. In this context, a POSITA would not have been motivated to implement Landi's non-compliant encrypted IDs in Dick's system as Datavant proposes, and Ground 3 should thus be rejected in its entirety. EX2001, ¶¶169-173, 195-198.

In addition, and apart from the combinability of the references, the

produced healthcare information including the encrypted IDs in the Dick-Landi combination fail to meet the requirement of dependent claims 2, 8, and 15 to be in conformity with HIPAA.

3. The Reply Continues to Rely on Impermissible Hindsight in Arguing that it Would Have Been Obvious to Transform Dick's Requester's Server into an Encryption Server that Produces Tokens for Individuals Identified in the Request

Neither Dick nor Landi describes an encryption server that produces tokens for individuals identified in a request for healthcare information, as Vigilytics explained in the POR. POR, 56-58. Datavant does not dispute this in the Reply, but instead resorts to the same hindsight-driven obviousness arguments from the Petition in which it manufactures a supposed need for such tokens based on an alleged desire to search for individual patients' records in the central database based on encrypted ID. Reply, 21; Pet., 36-37, 41-42. This argument fails for the reasons detailed in the POR, including that:

- Neither Landi nor Dick contemplate searching by encrypted IDs in the manner required by the combination;
- The combination imagines distributing keys needed to a non-covered entity under HIPAA (e.g., Dick's requester's server) to generate encrypted IDs despite no suggestion for the same in Dick or Landi; and
- The combination imagines transforming Dick's requester server into a server that is capable of identifying patients without

authorization in violation of the patients' privacy rights and HIPAA.

POR, 53-59.

EX2001, ¶¶175-194; *see also id.*, ¶¶153-162.

D. Ground 4 – Dick in view of Landi and Murphy

Murphy does not “block queries” as Datavant contends. Pet., 69; Reply, 24-25. Murphy always answers the query with an obfuscated indication of the number of hits identified in response to the query—regardless of whether the number of hits is less than, equal to, or greater than a minimum number. POR, 66-68; EX2001, ¶¶201-202. Indeed, when that number is less than a minimum (e.g., < 3), Murphy answers with a range for the obfuscated number of hits, and Murphy otherwise answers with a single obfuscated value. EX1009, 555; *see also id.*, 553-556. Dr. Clark acknowledged the same, confirming that Murphy answers with obfuscated results in either case, contrary to Datavant's position. EX2008, 75:20-77:18.

III. CONCLUSION

The Challenged Claims have not been shown to be unpatentable and their patentability should be confirmed over Grounds 1-4.

Respectfully submitted,

Dated 01/27/2025

/Nicholas W. Stephens/

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

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

Nicholas Stephens, Reg. No. 74,320

Fish & Richardson P.C.

60 South Sixth Street, Suite 3200

Minneapolis, MN 55402

T: 202-783-5070

F: 877-769-7945

Attorneys for Patent Owner

CERTIFICATION UNDER 37 CFR §42.24(d)

Under the provisions of 37 CFR §42.24(d), the undersigned hereby certifies that the word count for the foregoing Patent Owner's Sur-Reply totals 5,593, which is less than the 5,600 allowed under 37 CFR §42.24(c)(4).

Respectfully submitted,

Dated 01/27/2025

/Nicholas W. Stephens/
W. Karl Renner, Reg. No. 41,265
Jeffrey J. Barclay, Reg. No. 48,950
Nicholas Stephens, Reg. No. 74,320
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Patent Owner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§42.6(e), the undersigned certifies that on January 27, 2025, a complete and entire copy of this Patent Owner's Sur-Reply and Exhibit 2008 were provided by email to Petitioner by serving the correspondence email address of record as follows:

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

E-mail: Datavant-IPRs@Venable.com

/Diana Bradley/

Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
bradley@fr.com