UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DATAVANT, INC.,
Petitioner,

v.

VIGILYTICS LLC,
Patent Owner.

Case IPR2024-00381
Patent 10,886,012 B1

PATENT OWNER'S SUR-REPLY

TABLE OF CONTENTS

I. Introduction.....1

II. Ground 2: The Evenhaim-Settimi-Murphy Combination is Deficient 1

A. The Combination is Rooted in Impermissible Hindsight.....1

1. The Reply Fails to Demonstrate a Motivation to Modify Evenhaim to Search De-Identified Medical Data, Which Teaches Away From the Same 2

2. The Combination Breaches Patient Privacy and Invites HIPAA Violations by Granting a Single Entity Access to Both (i) Personally Identifying Information for Patients in the Group and (ii) De-Identified Medical Records for Patients in the Group 9

3. The Combination's Reliance on Settimi's EPIDs is Illegal under HIPAA and Non-Obvious 13

B. The Combination Fails to Disclose or Render Obvious Multiple Limitations of the Challenged Claims.....19

III. Ground 1: The Evenhaim-Murphy Combination is Deficient 22

A. The Combination Fails to Disclose or Render Obvious Multiple Limitations of the Challenged Claims.....22

IV. Ground 3: The Dick-Landi-Murphy Combination is Deficient.....25

A. The Combination is Rooted in Impermissible Hindsight.....25

1. The Combination's Reliance on Landi's Encrypted IDs is Illegal under HIPAA and Non-Obvious 25

2. The Combination Breaches Patient Privacy and Invites HIPAA Violations by Granting a Single Entity Access to Both (i) Personally Identifying Information for Patients in the Group and (ii) De-Identified Medical Records for Patients in the Group 26

B. The Combination Fails to Disclose or Render Obvious Multiple Limitations of the Challenged Claims.....28

V. Conclusion 29

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, IPR2024-00226, September 26, 2024
2009	Transcript of Deposition of Paul C. Clark, March 20, 2025

I. INTRODUCTION

The Reply fails to show that any claim of the ’012 Patent is unpatentable. Even with the benefit of Vigilytics’ earlier arguments on similar issues in IPR2024-00226, Datavant continues to advance arguments in defense of prior art combinations that would be illegal under HIPAA and that a POSA would not find obvious to pursue. More, and apart from critical flaws in its combination theories, Datavant is still unable to show that the prior art, even if combined, would disclose or render obvious a range of claim features.

For the reasons described in further detail below and in the POR, the patentability of all claims of the ’012 Patent should be confirmed.

II. GROUND 2: THE EVENHAIM-SETTIMI-MURPHY COMBINATION IS DEFICIENT

A. The Combination is Rooted in Impermissible Hindsight

Datavant’s Reply maintains that a POSA would find it obvious to combine Evenhaim, Settimi, and Murphy to arrive at the claimed inventions of the ’012 Patent, but in so doing, the Reply disregards multiple problems that are strongly indicative of impermissible hindsight. Among other things, for example, Evenhaim explicitly instructs a POSA ***not*** to search de-identified medical records. Datavant then advances illogical claims that a POSA would be motivated to integrate features in the combination that would risk identifying patients’ private health information without authorization, and that would be illegal under HIPAA.

Against this record, Datavant has not shown that the combination is anything more than the byproduct of impermissible hindsight. *Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc.*, 711 F.3d 1348, 1368 (Fed. Cir. 2013) ("[T]he prejudice of hindsight bias often overlooks that the genius of invention is often a combination of known elements which in hindsight seems preordained."). Ground 2 thus fails from the outset for each of the reasons described below.

1. The Reply Fails to Demonstrate a Motivation to Modify Evenhaim to Search De-Identified Medical Data, Which Teaches Away From the Same

The Reply fails to establish that a POSA would be motivated to modify Evenhaim based on Settimi to search de-identified healthcare information. As explained in the POR, the proposed modification violates Evenhaim's principle of searching raw, high-resolution healthcare information ***before de-identification***. POR, 30-31, 48-49; EX2001, ¶¶120, 142-143. Datavant argues that the combination does not "violate" Evenhaim's teachings, but even if this were true (it is not), the mere absence of a violation does not show that a POSA ***would*** be motivated or capable of turning from Evenhaim's original solution in the first instance. *See* Reply, 6-7; *InTouch Techs., Inc. v. VGO Commc'ns, Inc.*, 751 F.3d 1327, 1352 (Fed. Cir. 2014) (finding error in obviousness arguments that "primarily consisted of conclusory references to [a] belief that one of ordinary skill in the art ***could*** combine these references, not that they ***would*** have been

motivated to do so") (emphasis in original).

Recall that, in the combination, Datavant proposes modifying Evenhaim's system such that the data aggregator would search Settimi's central repository of de-identified records rather than searching original patient records at the data source entities (*e.g.*, healthcare provider sites). Pet., 37-40. The only reason Datavant offers for de-identifying the patient records before searching is to "reduc[e] the risk of a HIPAA violation." Pet., 40. While Datavant separately contends that consolidating patient records in a central repository would be useful to "make[] searching easier and more reliable" by "eliminat[ing] the need for conducting searches across different entities," the alleged desire to reduce risk of HIPAA violations constitutes the entire rationale given for modifying Evenhaim to search de-identified records. But this motivation is illusory since Evenhaim's search of original patient records at the data source entities already poses no HIPAA issues—a fact that Datavant has never disputed. *See, e.g.*, Pet., 15 ("Evenhaim is intended to comply with the provisions of HIPAA.").

Compounding this problem, Datavant never reconciles its proposal to search de-identified data with Evenhaim's express goal of searching original, high-resolution records ***before de-identification***. EX2001, ¶¶120, 142-143. Even if the patient records were required to be de-identified before their release to the central repository to comply with HIPAA, the Reply cites ***no*** evidence that the

speculative efficiency gains flowing from a centralized search would have justified the high cost that Evenhaim attributes to searching de-identified medical records as opposed to the original records in their most complete form. The law is clear that a motivation cannot be established through evidence that disregards the express preferences of a reference as Datavant does here. *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1069 (Fed. Cir. 2018) (explaining that "statements regarding preferences are relevant to a finding regarding whether a skilled artisan would be motivated" and that "by completely disregarding certain teachings as ill-defined 'subjective preferences,' the Board's approach invited the 'distortion caused by hindsight bias' into the fold").

To be sure, Evenhaim's aversion to searching de-identified data is unambiguous and reflected by strong language rarely seen in patent literature. According to Evenhaim, "[t]he challenge of measuring the impact of a consumer health program becomes significant whenever the health program sponsor does not have the ***full healthcare information*** of the target population at their disposal." EX1005, 4:35-39[1]. Evenhaim further observed that existing models that relied on de-identified data for longitudinal searches were inadequate because "[o]ne cannot query or analyze parameters that are ***no longer in the lower***

[1] All emphasis added unless otherwise indicated.

resolution database" (*see* 16:63-64), especially as such models "preclude[] external researchers from benefiting from the ***richness of the 'source-entity' data***." *Id.*, 16:63-64, 7:46-52. Because de-identification methods involve stripping identifying information from the original patient medical records, de-identification necessarily produces a lower resolution dataset that lacks the same richness of the original data—a fact that even Dr. Clark could not deny. EX2009, 72:22-73:6; EX2006, 1-2; 45 C.F.R. § 164.514(b)(2) (describing de-identification methods under HIPAA that involve stripping PII); EX2008, 20:8-20:23. Consistent with his overarching concern over the loss of any data/parameters from the original dataset, Evenhaim does not mince words in expressing his disdain for searching de-identified data stripped of PII:

> HIPAA provides substantial limitation on Personal Health Information and ***existing de-identification method may render the information <u>useless</u>*** for the purpose of measuring the impact of health programs.

EX1005, 4:42-45.

Underscoring this point, Evenhaim explicitly contrasts his approach to searching original, high-resolution data at the data source entities with other models that required the search to be performed on de-identified data—*i.e.*, the same technique that Datavant proposes to apply in the combination:

<u>Approach Disparaged by Evenhaim:</u>	**<u>Evenhaim's "Crossix" Method:</u>**

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.

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.*, 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 further explains that an important reason his system performs the "opposite sequence" of searching before de-identifying rather than the "classic" model of de-identifying before searching is that it was impossible to match a specific group of individuals to their corresponding medical records once they had been de-identified according to any existing/known solutions at the time:

Most existing analytics services in healthcare are based on a model where patient-level health transactions are de-identified and then aggregated and processed for analysis. Clearly through this process, high-resolution raw data that includes the maximum amount of information is reduced to a lower resolution data to preserve privacy and possibly other interests. Many companies, including IMS Health, Verispan (a joint venture between Quintiles and McKesson), Pharmetrics, Dendrite and others employee this model. This existing health analytics model may provide either physician level behavior or de-identified patient-level behavior and possibly a combination of both. However, while this model is very effective in analyzing longitudinal patient behavior and, in some cases, matching it to a known prescriber (such as physician), no linkage can be made to a consumer health program that only impact a subset of the market (unless the program correlate well with a limited region or cover a known group of physicians). One cannot query or analyze parameters that are no longer in the lower resolution dataset. Therefore, the existing healthcare analytics model does not provide the capability to aggregate the behavior of a group of patients by a predefined list of consumers participating in a health program.

EX1005, 16:45-67. Unlike Mr. Paris, inventor of the Vigilytics patents, Evenhaim never figured out how to search/analyze healthcare information for a specific group of individuals from a set of ***de-identified*** data. Evenhaim instead required the search to be performed on original, non-de-identified data at the data source entities because that was the only way Evenhaim found that medical records associated with particular individuals could be matched. *Id.* It was not obvious to Evenhaim how to use tokens or any other allegedly well-known techniques to enable searching for a specific group of individuals on de-identified data; Evenhaim instead proposed an entirely different solution than the '012 Patent squarely at odds with the combination proposed in Ground 2. EX2009, 70:7-11, 39:18-40:11.

Evenhaim's own writing shows that Datavant's combination is borne of impermissible hindsight rather than any legitimate aspirations of a POSA before the '012 Patent, for the reasons discussed above. And while the Board need not reach the issue to find the combination deficient, the record amply shows that Evenhaim teaches away from the combination, especially considering Evenhaim's repeated criticisms of de-identified data. *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."); POR, 30-31, 48-49; EX2001, ¶¶120, 142-143.

Datavant's contention that Evenhaim does not teach away from the combination also is not credible as Datavant simply refuses to acknowledge the portions of Evenhaim that cut against its narrative. For example, the Reply never addresses Evenhaim's characterization of de-identified data as "useless" and never addresses Evenhaim's broader teachings that show his concern with data loss was not limited to aggregating data at the physician-level or around large cluster variables. Dr. Clark was so obstinate during his deposition that he refused even to acknowledge that Evenhaim's description of de-identified data as "useless" constituted any criticism or preference whatsoever. EX2009, 73:7-75:20.

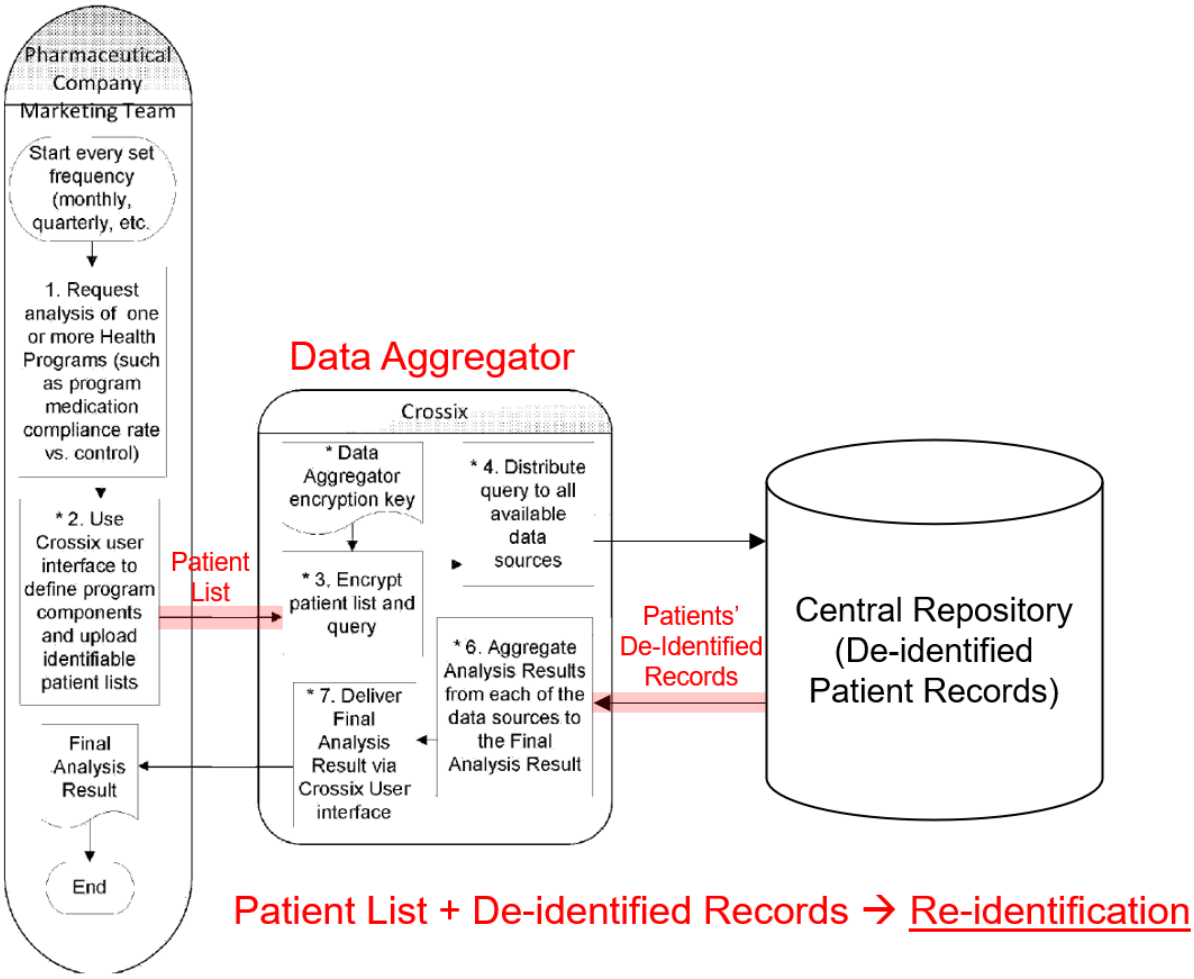
Datavant also misrepresents Evenhaim in arguing that its data sets "are not harmed by the removal of PII inasmuch as Evenhaim acknowledges the option of '*identity-free* micro-data." Reply, 7-8. Evenhaim's mention of "identity-free micro data" is in reference to data that has been de-identified ***after*** the search, which is not how the Evenhaim-Settimi-Murphy combination purportedly operates. EX1005, 10:29-41. Datavant's additional suggestion that Evenhaim actually contemplated searching de-identified data because "Evenhaim describes searches in which the patient is identified other than by his/her name" is also a red herring. Reply, 7. Merely because identifiers other than a name can be used to

uniquely resolve a patient's medical record does not imply that the source data is de-identified; on the contrary, it suggests that the source data is robust and contains the full healthcare information for the patient such that flexibility in the search query can be accommodated by a variety of identifiers. EX1005, 8:30-34.

2. The Combination Breaches Patient Privacy and Invites HIPAA Violations by Granting a Single Entity Access to Both (i) Personally Identifying Information for Patients in the Group and (ii) De-Identified Medical Records for Patients in the Group

The Reply next fails to refute Vigilytics' showing that the Evenhaim-Settimi-Murphy system exhibits a critical security flaw that a POSA would never tolerate, let alone pursue. POR, 26-27, 29-30, 59-60; EX2001, ¶¶114, 119, 156. Specifically, the combination calls for Evenhaim's data aggregator to receive two pieces of information that together can be used to reverse engineer patient identities in contravention of basic privacy norms and HIPAA—namely, (i) personally identifying information (PII) for the group of patients whose medical data is to be searched (which the aggregator uses to issue a search query) and (ii) de-identified medical records for patients in the group (which are returned to the aggregator as search results). Pet., 39-44; EX1004, FIGS. 4-4A. Combining these two pieces of information is problematic because it allows the entity in possession of them both to match the de-identified records to specific patients, thus exposing the patients' protected health information without authorization. EX2001, ¶¶114,

119, 156.



Evenhaim-Settimi-Murphy Illustration

The ’012 Patent specifically recognized this problem and provided solutions to address it by isolating both pieces of information and ensuring that no single entity accesses both the list of individuals in the group and their de-identified medical records:

By using the tokens **202** and request tokens **204**, no parties other than the authorized source sites **138** can associate de-identified data **140** with the identity of any person in the group of patients **134** or insureds (e.g., the group **154**). The insurer **150** requesting the report **212** can never receive data associated with individuals. Further, the information in the report **212** may be processed into metrics that characterize a large group and cannot be used to infer information about individuals. De-identified data records may be provided to the data processor **210** (e.g., a third part data processor), but that third party may not have access to any personally identifiable information **118** about the group **154**. Nor may any party with access to the de-identified data **140**, other than the healthcare providers **138**, also have access to the de-identifier **142**. These features of the system **200** maintain the privacy of the protected health information **130**.

EX1001, 4:54-5:3; *see also id.*, FIGS. 2-3 (isolating PII from de-identified records to preserve patient privacy).

Unlike the '012 Patent, the system in the Evenhaim-Settimi-Murphy combination does not isolate the identifying information for the patients in the group from the de-identified medical records. The peril in Datavant's approach was underscored by Dr. Clark when he conceded at his deposition that he "wouldn't recommend [that] anyone" make "names and health conditions available to someone that was not a covered entity." EX2009, 30:14-31:25; *see also id.*, 31:18-21 ("That wouldn't be the way I would implement the system" because "there would be a risk" of breaching the patient's privacy.), *id.*, 32:4-8 ("you would not want the names available"). Dr. Rubin agrees. EX2001, ¶¶114, 119, 156.

Datavant's various attempts to dismiss or workaround the security flaw are

all wrong or ineffective. Reply, 8-13. For instance, Datavant contends that "the '012 Patent's design would be subject to the same type of attack inasmuch as the token generator 314 at the encryptions server is not part of any closed off healthcare system." Reply, 8. This is wrong—the token generator 314 never receives de-identified medical records like the data aggregator in the Evenhaim-Settimi combination. *See* EX1001, FIG. 3. Datavant also argues that there would be no HIPAA violation because "Evenhaim and Settimi are directed to *achieving* HIPAA compliance." Reply, 9 (emphasis in original). But this argument ignores that the security flaw stems from the new function of the data aggregator that emerges ***in the combination*** as opposed to its original function in Evenhaim alone. Datavant constructed a new system in the combination that bears little resemblance to the systems of either Evenhaim or Settimi alone.

Datavant's additional suggestions for using Evenhaim's "escrow agent" to manage encryption keys on behalf of the data aggregator or to employ allegedly "well-known cryptographic methods" to block plain-text attacks are likewise ineffective, and they miss the nature of the re-identification risk altogether. *See* Reply, 10-11. Evenhaim explains that the "escrow agent" is merely a "trusted third party" that issues encryption keys. EX1005, 12:61-66. Datavant cites no evidence that an escrow agent would ever perform de-identification or receive PII on behalf of a data aggregator as suggested in the Reply. *Id.* Moreover, whatever

cryptographic countermeasures may stem a plain-text attack, they do not address the more fundamental problem that patients can still be re-identified by combining the patient list with the de-identified records alone—even if a matching token were not returned to the data aggregator due to the cryptographic countermeasures.

Likewise, Datavant's observation that returned medical records would be de-identified in accordance with HIPAA is immaterial. Reply, 11-13. The security vulnerability in the proposed combination flows from the ability to correlate the identities of the patients in the list with the healthcare information contained in the patients' medical records. This problem persists even when the medical records have been de-identified in accordance with HIPAA, as recognized in the '012 Patent. EX1001, 4:54-5:3.

3. The Combination's Reliance on Settimi's EPIDs is Illegal under HIPAA and Non-Obvious

Datavant's Reply next fails to show that the proposed use of Settimi's encoded patient identifiers (EPIDs) for searching de-identified medical records in Evenhaim's system would be obvious.[2] This aspect of the combination fails for at

[2] The Petition and Dr. Clark relied on Settimi's EPIDs in the Evenhaim-Settimi-Murphy combination. Pet., 38, 45; EX1015, ¶12 (alleging that "a POSA would

least three reasons.

First, Settimi's EPIDs violate HIPAA when disclosed outside a covered entity, and a POSA would not seek to implement an illegal system. Section 164.514(c) of the HIPAA Privacy Rule prohibits any "code or other means of record identification" disclosed by a covered entity from being "derived from or related to information about the individual." EX2006; EX1025, 79:6-84:9; POR, 55-56. Settimi's EPIDs, however, are specifically derived from patients' personally identifying information in their medical records. For example, Settimi explains that the EPID can be generated from the patient's name, age, social security number, patient identifier (PID), or combinations of identifiers—all of which Dr. Clark agreed constitutes PII. EX1006, [0041]; EX2009, 64:12-23. Settimi's EPIDs thus directly violate the Privacy Rule's restrictions on deriving identification codes from PII. Dr. Clark had no choice but to concede under cross-examination that "generally speaking" an identification code derived from PII is

---

have found it logical (and obvious) to search in Settimi's centralized database using EPIDs").

not compliant with the derivation provision. EX2009, 55:1-3, 53:20-55:3.[3]

While HIPAA does not preclude the use of hash functions to generate identification codes from PII (since the hash irreversibly deidentifies the PII), ***reversible*** encryption using conventional symmetric/asymmetric cryptography is nonetheless impermissible. EX1016, 30-31. Contrary to assertions in the Reply, however, Settimi's EPIDs are ***always*** reversibly encrypted; the patient's PII is never hashed in Settimi when generating an EPID. This is not an accident or a mere design choice. Settimi uses reversible encryption techniques specifically to ensure patients can be re-identified through decryption of EPIDs by the PCPs. EX1006, [0027] ("re-identified at the PCP"), [0037], [0041]-[0048].

Datavant contends that "Settimi's method" involves "encrypting patient identifying information with, *e.g.*, a hash function" but this is not true. Reply, 12. Settimi's only mention of a hash is with respect to the "encoded password string." EX1006, [0041]. By contrast, Settimi discloses reversible encryption algorithms such as "[t]he two-fish algorithm" or the "Rivest, Shamir, and Adelman, RSA

[3] Dr. Clark similarly testified in IPR2024-00226 involving a related Vigilytics patent that an identification code derived from PII "[s]trictly speaking[] … would not be compliant with the derivation requirement." IPR2024-00226, EX2008, 71:6-13.

algorithm" (not a hash) to encrypt the PII. *Id.*; EX2009, 66:22-67:19. Settimi's reversible encryption of PII amounts to a plain HIPAA violation that would have deterred a POSA from making the combination.[4] EX2006; EX2009, 53:20-55:3.

Datavant's effort to excuse Settimi's reversible encryption also fails. For example, Datavant contends that the Privacy Rule does not forbid "an encryption technique that allows for decryption," and cites guidance from the U.S. Department of Health and Human Services ("HHS Guidance") in support of this argument. Reply, 19 (citing EX1016, 30-31). But Datavant misrepresents the HHS Guidance, "stat[ing] that the re-identification provision 'does not preclude' 'cryptographic' options." *Id.* Not true. The ***only*** suitable "cryptographic" option

[4] The parties do not dispute that the '012 Patent is directed to methods/techniques for HIPAA compliance. EX1001, 1:18-40, 4:5-10; POR, 12; EX2001, ¶¶72-73; EX1025, 76:12-79:5, 75:19-76:14 (Dr. Rubin explaining that HIPAA is an integral backdrop to the invention); EX2009, 13:18-44:15, 17:10-18; Pet., 2-7. Moreover, HIPAA compliance is relevant to whether a POSA would have been motivated to implement the proposed combinations because the primary references in the instituted grounds, Evenhaim and Dick, were likewise concerned with HIPAA compliance—*i.e.*, a fact that Datavant even touted in the Petition to support its own motivations to combine. Pet., 56, 40, 60-62.

identified in the HHS guidance is an irreversible hash function. EX1016, 30-31.

Datavant also alleges that the ’012 Patent “acknowledges reversible encryption,” but this too is misleading. Reply, 5 (citing EX1001, 7:42-46). The portion of the specification Datavant cites refers to “unencrypt[ing]” a request message or a batch file, but in no case are the request tokens themselves decrypted. *Id.*; EX1001, 6:37-47, 7:35-41; EX2009, 33:8-34:8, 45:1-14. Nor could tokens be decrypted in the ’012 Patent because the tokens are ***irreversibly*** de-identified. EX1001, 5:44-51, 6:6-9, 4:5-10; EX2009, 48:15-22; EX1025, EX1025, 79:6-84:9.

Second, contrary to assertions in the Reply, the use of EPIDs for searching the central database is entirely unsupported by Settimi. As explained in the POR, Settimi describes methods for searching the central database 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, 44-48. Settimi never contemplates searching the central database by EPIDs. *Id.*

The Reply contends that the disclosure at paragraph 47 of Settimi provides a relevant EPID-based search, but this too is wrong. Reply, 5-6. Paragraph 47 only describes the ability of a user to enter an EPID ***in the PCP’s local electronic medical records (EMR) system***. 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*** …"). Settimi never describes functionality for searching the central warehouse using EPIDs. The new use of EPIDs for searching the central warehouse was simply manufactured by Datavant using the claims of the '012 Patent as a roadmap.

Third, Evenhaim's data aggregator would be incapable of producing 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 a PCP can generate an EPID because it requires encrypting PII such as a patient identifier (PID) and 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]. The data aggregator in the Evenhaim-Settimi combination would lack the inputs such as the password string necessary to produce an EPID for searching the central database, and significantly, disclosure of the keys necessary for the data aggregator to generate an identification code like an EPID would violate §164.514(c)(2) of the HIPAA Privacy Rule. EX2006, 2-3 (45 C.F.R. § 164.514(c)(2)); EX1016, 30-31 ("provided the keys associated with such [cryptographic hash] functions are not disclosed, including to the recipients of the

de-identified information"); EX2001, ¶¶151.

B. The Combination Fails to Disclose or Render Obvious Multiple Limitations of the Challenged Claims

[1.e]-[1.f] – "the unique tokens associated with healthcare data are absent identities of individuals"; "the identity of the individuals being unattainable from the produced healthcare information"

Datavant contends that the identity of the individuals is "unattainable" from Settimi's EPIDs (which are part of the produced information in the combination), and argues with respect to similar features in Ground 3 that the identity of an individual corresponding to reversibly encrypted PII is rendered unattainable "by protecting the decryption key." Reply, 23; EX1006, [0027] ("re-identified at the PCP"), [0037], [0041] ("symmetric encryption"), [0042]-[0048]. Datavant likewise argues that Settimi's EPIDs are "absent" PII. But the claims do not condition the claimed unattainability or absence of PII to only those entities that lack a decryption key. POR, 65-66. The '012 Patent instead distinguishes reversibly encrypted information for which the identities of individuals remain attainable from irreversibly deidentified information for which the identities of individuals are unattainable. EX1001, 6:41-43, 3:49-53, 6:18-35 (differentiating reversibly encrypted request message 306 carrying PII from irreversibly deidentified data 140/204/212); EX2009, 46:16-48:14 (Dr. Clark describing difference between reversible encryption and irreversible de-identification). Evenhaim-Settimi-Murphy thus fails to disclose or render obvious [1.e]-[1.f].

[1.b], [1.d] – "the encrypted request message including a unique token produced … for each individual in the group"; "the server is configured to compare the unique request tokens to unique tokens associated with healthcare data to find matching tokens"

Datavant is still unable to show in the Reply any prior art that produces a request token for each individual identified in a request for healthcare information, and that then compares the request tokens to tokens associated with de-identified data to find matching tokens, as recited in [1.b], [1.d]. To this point, Evenhaim does not rely on matching tokens in this manner but instead searches original patient data before de-identification. *Supra*, §II.A.1; POR, 30-34. Settimi's central database is likewise deficient since it is queried by demographic or clinical criteria to identify patient cohorts and is never queried by tokens to identify medical records for a specific group of patients.[5] *Supra*, §II.A.3; POR, 46-48. Lacking any express disclosure of these features, Datavant resorts to uncorroborated assertions that it would nonetheless be obvious for "the patient records [to] be queried using tokens because tokens (*e.g.*, 'EPIDs') are the only language Settimi's centralized database understands for identifying records." Reply, 4-5. But obviousness can only be used to supply missing claim limitations

[5] Datavant does not rely on Murphy for these limitations, although it too is inapplicable.

when the limitations at issue are uncommonly simple and the technology straightforward, and here, the issue of how to securely produce tokens that could be matched against de-identified data while protecting patient privacy and complying with HIPAA is anything but simple or straightforward. *Supra*, §II.A.3; *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1362 (Fed. Cir. 2016) ("[O]ur cases repeatedly warn that references to 'common sense' … cannot be used as a wholesale substitute for reasoned analysis and evidentiary support, especially when dealing with a limitation missing from the prior art references specified"). Tellingly, despite alleging that "token-matching" in this context was well known, Datavant has identified ***no prior art that actually discloses these features***. Dr. Clark further admitted that, not only had he never implemented an expert system in the healthcare field, but he was also unaware of any prior art systems that disclosed these features. EX2009, 39:18-40:11, 70:7-11.

[1.g]-[1.h] - "receiving, at the user computing device, the produced healthcare information to report the characteristics of the group absent authorization from the individuals in the group"

Evenhaim explains that the patients identified in its requests for healthcare information are individuals who "opt-in" to participate in a health program. EX1005, 15:34-36 ("These pharmaceutical health programs are promoted to consumers of that product who ***opt-in*** to participate in the program. The participants of each program ***allow[] … the pharmaceutical manufacturer to***

analyze their data in aggregate."), 5:46-59 ("opt-in"), 15:25-45. According to Dr. Clark, "opt[ing] into a health program" "means to agree to participate," and Dr. Clark agreed that a patient who opts-in to a health program authorizes use of their healthcare information for the program. EX2009, 77:3-77:18. Because the patients in Evenhaim's system, and thus in the combination, authorize use of their healthcare information in the health program, the healthcare information is not produced "***absent authorization*** from the individuals in the group" as recited in [1.g]-[1.h].

[2] - "the provided healthcare information is in conformity with [HIPAA]"

As discussed above, it would not be obvious to combine the teachings of Evenhaim, Settimi, and Murphy at least because the resulting system would violate HIPAA. *Supra*, §II.A.2-3. It follows that the system in the combination would not provide healthcare information in conformity with HIPAA as recited in claim 2.

III. GROUND 1: THE EVENHAIM-MURPHY COMBINATION IS DEFICIENT

A. The Combination Fails to Disclose or Render Obvious Multiple Limitations of the Challenged Claims

Ground 1 based on the Evenhaim-Murphy combination fails for many of the same reasons as those discussed above with respect to Ground 2 and in further detail in the POR. *Supra*, §II; POR, 13-44. Datavant's reliance on Evenhaim in

Ground 1 is indeed fundamentally flawed because Evenhaim does not search ***de-identified*** healthcare information, which Datavant has argued in an attempt to show that Evenhaim's data aggregator would produce and match tokens associated with healthcare data that do not reveal the identities of individuals. Pet., 16-26. Evenhaim instead specifically sought to "allow analysis of 'source-entity' ***raw data*** at is [sic] ***original***, most detailed form"—i.e., before the data is de-identified. EX1005, 6:15-17; *see also id.*, 4:42-45 ("de-identification method[s] may render the information ***useless*** for the purpose of measuring the impact of health programs"), 16:64-67 (existing models using de-identified data "***do[] not provide the capability*** to aggregate the behavior of a group of patients by a ***pre-defined list*** of consumers"), 16:49-17:3. Evenhaim thus explicitly contrasted his approach to searching the original data at the data source entities to prior models that de-identified and aggregated patient medical data ahead of time:

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.

The Reply offers no credible answer and fails to cure this basic deficiency

in Evenhaim's disclosure. Datavant instead buries its arguments on Ground 1 behind Ground 2 in the latter half of the brief. Reply, 13-17. Datavant cites Evenhaim's mention of "identity-free micro-data," but as explained above, this disclosure pertains to micro-data that has been de-identified ***after*** the original (non-de-identified) is searched. *Supra*, §II.A.1; EX1005, 10:29-41, 12:36-67, 6:64-7:26, FIG. 3. Because Evenhaim's system does not search de-identified data, it has no need to, and does not, produce tokens for the individuals in the request or match request tokens to corresponding tokens associated with de-identified data. POR, 16-34; EX2001, ¶¶101-136. The Reply attempts to stretch Evenhaim's disclosure of encrypting patient lists and encrypting queries for transmission security to somehow inject tokenization in Evenhaim, but these efforts do not withstand scrutiny when considering the lack of any encryption of individual patient information (as opposed to encryption of entire patient lists), and the fact that the parameter lists are always decrypted before any searches at the data source entities are performed. *Id.*; EX1005, 13:33-36, FIG. 5 ("Decrypt"). Evenhaim thus fails to disclose [1.b] or [1.d].

Beyond these deficiencies, the Evenhaim-Murphy combination fails to disclose "receiving, at the user computing device, the produced healthcare information to report the characteristics of the group ***absent authorization*** from the individuals in the group," as recited in [1.g]-[1.h] for the reasons discussed

above with respect to Ground 2. *Supra*, §II.B. The parameters that Evenhaim uses to query for specific individuals also are not "***absent identities of individuals***" as [1.e] requires of the claimed "unique tokens." Evenhaim instead explains that the search parameters for individuals "include identity disclosing specifics—***which probably do not pass ordinary criteria of even nominal privacy thresholds***." EX1005, 8:4-9; *generally id.*, 7:64-48.

IV. GROUND 3: THE DICK-LANDI-MURPHY COMBINATION IS DEFICIENT

A. The Combination is Rooted in Impermissible Hindsight

1. The Combination's Reliance on Landi's Encrypted IDs is Illegal under HIPAA and Non-Obvious

Ground 3 is premised on Datavant's argument that it would be obvious for a POSA to use Landi's encrypted IDs to search a central repository of de-identified medical records in Dick's system. Pet., 54-59. It would not. Landi's encrypted IDs would be illegal under HIPAA when disclosed by a covered entity because they are (i) derived from patients' PII and (ii) reversibly encrypted. POR, 55-56; EX2001, ¶151; *see also* EX1008, 5:13-19 (Landi describing how encrypted IDs are reversibly encrypted forms of PII); EX2008 (HIPAA Privacy Rule § 154.514(c) forbidding re-identification codes from being derived from PII); EX1016, 30-31 (HHS Guidance); EX1025, 79:6-84:9. Both parties' experts agree. EX2001, ¶151; EX2009, 55:1-3, 53:20-55:3 (Dr. Clark conceding that

Landi is arguably not compliant).[6] Landi also describes no other option for generating encrypted IDs except by encrypting PII using reversible cryptographic methods, which is consistent with Landi's goal of permitting re-identification of patients through decryption of the encrypted IDs. EX1008, Abstract, 2:30-40, 3:42-52; Reply, 19-20.

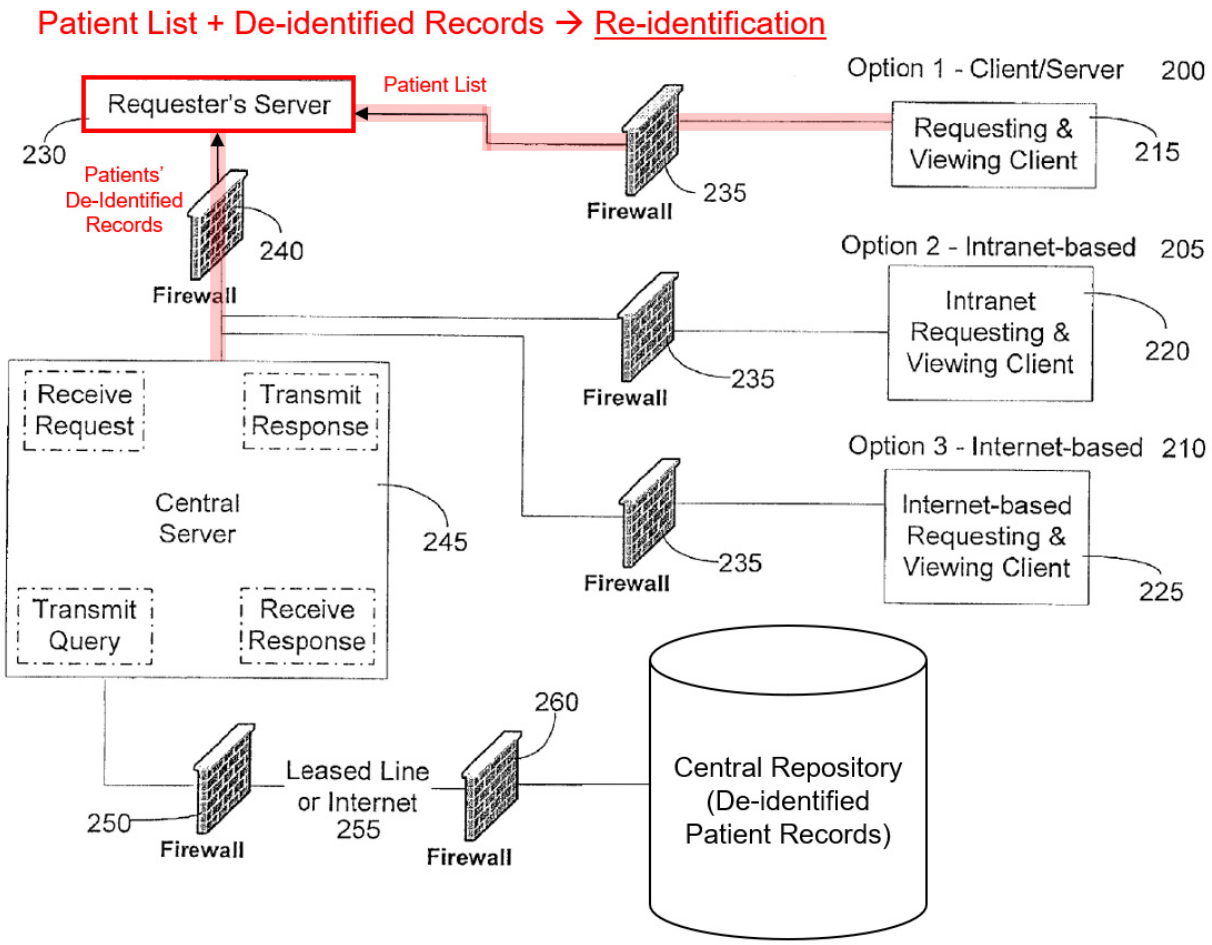
For reasons similar to those addressed in detail above (*supra*, §II.A.3), a POSA would not be motivated to implement features that violated HIPAA. This is clear from Datavant's own characterization of Dick's "purpose" as "compliance with HIPAA," and similarly, Datavant's own obviousness theories that cite HIPAA compliance as allegedly motivating the combinations in the first place. *See, e.g.*, Pet., 56, 40, 60-62; EX1003, ¶¶68-69, 86, 135, 136, 200, 213-214; EX2009, 13:18-44:15, 17:10-18 (Dr. Clark acknowledging importance of HIPAA compliance to a POSA).

2. The Combination Breaches Patient Privacy and Invites HIPAA Violations by Granting a Single Entity Access to Both (i) Personally Identifying Information for Patients in the Group and (ii) De-Identified Medical Records for Patients in the Group

The Dick-Landi-Murphy combination exhibits the same security flaw, and invites substantially the same HIPAA violations, as the Evenhaim-Settimi-

[6] *Supra*, Footnote 3.

Murphy combination described in detail above and in the POR. *Supra*, §II.A; POR, 59-60. In the combination, Dick's requester's server is configured to receive both PII for the group of individuals in the request and de-identified medical records for those individuals in response to the request. Pet., 54-59. This architecture would allow the entity that operates the requester's server to re-identify patients by correlating the de-identified records with the PII for the individuals in the group, which is precisely what the '012 Patent warns must not be done. EX1001, 4:54-5:3; *see also id.*, FIGS. 2-3. HIPAA does not allow patient's healthcare information to be released if it can be combined with PII to re-identify patients, and a POSA would not have implemented a system that jeopardized patient privacy or so blatantly risked HIPAA violations as the system in the Evenhaim-Settimi-Murphy combination. EX2006, 1-3; EX2001, ¶114, 119, 156. This was underscored by Dr. Clark's admission that "[t]hat wouldn't be the way I would implement the system." EX2009, 30:14-31:25.



Dick-Landi-Murphy Illustration

B. The Combination Fails to Disclose or Render Obvious Multiple Limitations of the Challenged Claims

Even if Datavant could establish that a POSA would have motivation to combine Dick, Landi, and Murphy (which it cannot), the resulting combination would still fail to disclose multiple features of the Challenged Claims.

For example, Ground 3 relies on Murphy for producing healthcare information "***based on a minimum number of matched tokens***," as recited in [1.f], but Murphy is deficient on this feature for the reasons described in detail in

the POR. POR, 66-69.

Datavant contends that Landi's encrypted IDs are absent identities of individuals and that the identities of individuals are unattainable from the encrypted IDs (which is included among the produced healthcare information in the combination) as recited by [1.e]-[1.f]. Reply, 23-24. But the claims do not condition the claimed unattainability or absence of PII to only those entities that lack a decryption key. POR, 65-66; EX2001, ¶¶165-166. The '012 Patent instead distinguishes reversibly encrypted information for which the identities of individuals remain attainable from irreversibly deidentified information for which the identities of individuals is unattainable. EX1001, 6:41-43, 3:49-53, 6:18-35 (differentiating reversibly encrypted request message 306 carrying PII from irreversibly deidentified data 140/204/212); EX2009, 46:16-48:14. Element [1g] has therefore not been shown to be obvious. The Reply likewise fails to rebut Vigilytics' showing that Elements [1.b], [1.d], [2], or corresponding limitations in independent claims 7 or 14, are obvious.

V. CONCLUSION

The Challenged Claims have not been shown to be unpatentable and their patentability should be confirmed over Grounds 1-3.

Respectfully submitted,

Dated 03/26/2025

/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 5,555, which is less than the 5,600 allowed under 37 CFR §42.24(c)(4).

Respectfully submitted,

Dated 03/26/2025

/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 March 26, 2025, a complete and entire copy of this Patent Owner's Sur-Reply and Exhibit 2009 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