UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

DATAVANT, INC.

Petitioner

v.

VIGILYTICS LLC

Patent Owner

IPR2024-00381

U.S. Patent No. 10,886,012 B2

REPLY DECLARATION OF PAUL C. CLARK, DSC.

Datavant Exhibit 1015
Datavant v. Vigilytics
IPR2024-00381

TABLE OF CONTENTS

I. Introduction 4

II. Materials Considered 4

III. Legal Testimony 6

IV. Person of Ordinary Skill in the Art 6

V. Ground 2: Obvious (§ 103) over Evenhaim in view of Settimi and Murphy 7

A. Prior Art References 7

B. Settimi Suggests Various Search Options 9

C. Evenhaim's Preference is for a Robust Database 10

D. The Combination of Evenhaim and Settimi Would Not Violate HIPAA 11

E. Evenhaim and Murphy Suggest Using Minimums 15

VI. Ground 1: Obvious (§ 103) over Evenhaim and Murphy 16

VII. Ground 3: Obvious (§ 103) over Dick, Landi, and Murphy 18

A. Prior Art References 18

B. A POSA Would Be Motivated to Combine Dick and Landi 18

C. A POSA Would Not Understand Landi's Design to Violate HIPAA 19

D. The Application of Murphy 20

VIII. Conclusion 22

EXHIBIT LIST

Exhibit Number	Description
1001	U.S. Patent No. 10,886,012 (the "'012 Patent")
1002	File History of U.S. Patent No. 10,886,012
1003	Declaration of Dr. Paul Clark
1004	Curriculum Vitae Of Dr. Paul Clark
1005	U.S. Pat. No. 7,823,207 ("Evenhaim")
1006	U.S. Pat. Appl. Publ. No. 2007/0294111 ("Settimi")
1007	U.S. Pat. Appl. Publ. No. US 2002/0111833 ("Dick")
1008	U.S. Pat. No. 7,519,591 ("Landi")
1009	Shawn N. Murphy and Henry C. Chueh, *A Security Architecture for Query Tools used to Access Large Biomedical Databases*, 2002 AMIA Annual Symposium Proceedings, 552 (2002) ("Murphy")
1010	*Milliman, Inc. v. Gradient A.I. Corp.*, No. 1:21-Cv-10865-NMG (D. Mass.), Dkt. 108.
1011	*Credit Card Security: The Best Way to Secure Data is Not to Store the Data* (Hospitality Upgrade, Summer 2008, www.hospitalityupgrade.com)
1012	Jennifer G. Steiner, B. Clifford Neuman, and Jeffrey I. Schiller, *Kerberos: An Authentication Service for Open Network Systems*, Winter 1988 Usenix Conference (1988).
1013	Declaration of Sylvia Hall-Ellis, Ph.D.
1014	Transcript of the Deposition of Aviel D. Rubin from related IPR2024-00226
1016	*Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. Department of Health and Human Services, *available at*

	https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html
1020	*To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, U.S. Department of Health and Human Services, *available at https://privacyruleandresearch.nih.gov/pr_06.asp*
1021	37 C.F.R. § 160.103
1022	Provos & Mazieres, *A Future-Adaptable Password Scheme*, Proceedings of the FREENIX Track: 1999 USENIX Annual Technical Conference
1023	Morris & Thompson; *Password Security: A Case History*, 22 COMMUNICATIONS OF THE ACM 11 (1979)
1024	U.S. Pat. No. 7,668,820

I, Paul Clark, declare that:

I. INTRODUCTION

1. I have been retained by Venable LLP, counsel for Datavant, Inc. ("Datavant") to provide my opinions concerning the validity of claims 1-20 of U.S. Patent No. 10,886,012 ("the '012 Patent").

2. I am being compensated for my time at my normal consulting rate of $590.00/hour. This compensation does not depend on the nature or presentation of my testimony, or on the outcome of any proceeding.

3. In a prior declaration submitted in this case, I have set forth my opinions concerning claims 1-20 of the '012 Patent. Ex. 1003 ("Prior Declaration"). In particular, my Prior Declaration discussed that:

- Ground 1: Claims 1-20 are obvious over Evenhaim in view of Murphy;
- Ground 2: Claims 1-20 are obvious over Evenhaim in view of Settimi and Murphy; and
- Ground 3: Claims 1-20 are obvious over Dick in view of Landi and Murphy.

4. My Prior Declaration sets forth my qualifications.

II. MATERIALS CONSIDERED

5. I have reviewed, in addition to the materials listed in my Prior Declaration:

- Ex. 1016: *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. Department of Health and Human Services, *available at https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html*;
- Ex. 1020: *To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, U.S. Department of Health and Human Services, *available at https://privacyruleandresearch.nih.gov/pr_06.asp*;
- Ex. 1021: 37 C.F.R. § 160.103;
- Ex. 1022: Provos & Mazieres, *A Future-Adaptable Password Scheme*, Proceedings of the FREENIX Track: 1999 USENIX Annual Technical Conference;
- Ex. 1023: Morris & Thompson; *Password Security: A Case History*, 22 COMMUNICATIONS OF THE ACM 594 (1979);
- Ex. 1024: U.S. Pat. No. 7,668,820;
- Patent Owner Response;
- Ex. 2001: Expert Declaration of Aviel D. Rubin, Ph.D.;
- Ex. 2002: Transcript of Deposition of Paul C. Clark, September 26, 2024;

- Ex. 2003: Summary of HIPAA Privacy Rules (https://www.hhs.gov/sites/default/files/privacysummary.pdf)
- Ex. 2004: Summary of the HIPAA Security Rule (https://www.hhs.gov/hipaa/for-professionals/security/lawsregulations/index.html)
- Ex. 2005: HIPAA History (https://www.hipaajournal.com/hipaa-history/)
- Ex. 2006: 45 C.F.R. §164.514; and
- Ex. 2007: 45 C.F.R. §75.2.

III. LEGAL TESTIMONY

6. In expressing my opinions and considering the subject matter of the claims of the ’012 Patent, I am relying upon certain basic legal principles that have been provided and explained to me. Those principles are set forth in my Prior Declaration.

IV. PERSON OF ORDINARY SKILL IN THE ART

7. As stated in my Prior Declaration, I understand that an assessment of claims of the ’012 Patent should be undertaken from the perspective of a person of ordinary skill in the art as of the earliest claimed priority date, which I understand is July 1, 2009. I also understand that Vigilytics has generally agreed with

definition of a POSA in my Prior Declaration; however, Vigilytics asserts that the POSA would have had specific knowledge about medical databases and the manner of operating the same to comply with HIPAA. POR, 12-13 ("familiarity with medical records and databases for storing medical records—particularly in manner that complies with privacy laws and regulations such as HIPAA."). This additional knowledge for the POSA would make the subject matter claimed in the '012 Patent even more obvious to the POSA.

V. GROUND 2: OBVIOUS (§ 103) OVER EVENHAIM IN VIEW OF SETTIMI AND MURPHY

A. Prior Art References

i. Evenhaim

8. Evenhaim is directed to a system for searching for health records of specific patients in a manner that is HIPAA compliant. EX1005, 3:17-31, 4:1-3, 14:7-13, 4:34-48, 5:46-6:10, 8:18-22, 14:7-13, 14:59-67. As described in my Prior Declaration, in Ground 2, I rely upon on Evenhaim's search for a specific list of patients in combination with Settimi. Ex. 1003, ¶¶ 48, 136-39. Evenhaim discusses, in part, the preference for maintaining, for search purposes, micro-level data, as compared to earlier designs that provided what Evenhaim calls lower resolution databases. EX1005, 10:29-32, 12:36-52, 16:46-17:3, Fig. 4. Those earlier system designs discussed by Evenhaim would lump together data from

"larger cluster variable" such as age group, such that particulars for any one patient were no longer identifiable. EX1005, 7:46-52.

ii. Settimi

9. While Settimi states that "***[c]ertain embodiments*** provide systems and methods for searching electronic medical data to identify a pool of potential study participants" (EX1006, [0015][1]), the disclosure more "generally relates to search and analysis of electronic medical record data." EX1006, [0004]. Consequently, a POSA would understand that Settimi's teachings could be applied to a variety of types of searches by a variety of types of users. *Id.*, [0030] (users can be "from companies that make . . . other products").

10. Settimi uses a centralized data warehouse that excludes patient identifiers, *i.e.*, PII, in accordance with HIPAA. EX1006, [0009], [0017], [0027], [0035], [0060]. This is the same concept described in the '012 Patent, as shown for example in Fig. 3 of the '012 Patent. EX1001, 5:63-6:3, Fig. 3. In Settimi, the PII is replaced with an encoded patient identifier, referred to as an "EPID," that is created by using a hash function (or "[o]ther methods"), which is the same tokenization example offered in the '012 Patent (and Evenhaim). EX1006, [0038], [0041] ("hashes"); EX1001, 6:1-9; EX1014, 93:13-99:18. Unlike the types of low-resolution databases that Evenhaim discusses, Settimi's centralized warehouse

[1] Emphasis added throughout.

"retain[s] clinically useful information about the patient," including, for example, "dates of examination, documentation, diagnosis, prescription and lab test results." *Id.*, [0038], [0040].

B. Settimi Suggests Various Search Options

11. I understand that Vigilytics asserts that that Settimi should be understood to teach that queries are limited to one seeking patient "characteristics," as compared to searches for the records of particular patients. In particular, I understand that Vigilytics' position to be that Settimi would not suggest searching by EPID (*i.e.*, token) to a POSA. POR, 45-48. I disagree. Settimi makes clear that "[t]he user may search by the EPID number." *Id.*, [0047], [0050] ("Thus, broader analysis of patient information may be allowed, while at the same time respecting patient privacy."), [0051] ("Certain embodiments allow for patient information to be shared with interested parties without compromising patient privacy."), [0071], [0073]. Settimi also calls for searches of the user's own design. *Id.*, [0061].

12. Further, as discussed in my Prior Declaration, when looking for records for particular patients, a POSA would have found it logical (and obvious) to search in Settimi's centralized database using EPIDs because Settimi's database only identifies records by EPIDs (not names). *See* EX1003, ¶¶ 149-50. In this regard, Evenhaim teaches formatting the patient names provided by users into whatever terminology mutually agreed to by the aggregator and the source entities,

including "name or ID or the like[]." EX1005, 8:30-43, 49-55. Thus, Evenhaim's query would be formatted to match the token design used by Settimi's database, so that they speak the same language.

C. Evenhaim's Preference is for a Robust Database

13. Evenhaim's preference is simply for a robust set of data that would allow a user to search for, *e.g.*, patient records for a particular group of individuals. EX1005, 7:38-53. Specifically, as Evenhaim explains, lower resolution datasets were not preferred because they did not allow the systems to analyze "the behavior of a group of patients by a predefined list of consumers participating in a health program." *Id.*, 16:46-17:3, 3:32-53.

14. Settimi's centralized database preserves detailed medical records, while only tokenizing identifying information for those records to comply with HIPAA. EX1006, [0060]-[0061], [0063]. This allows for Evenhaim's goal because a database may be searched by EPID. *Id.*, [0047]. Thus, the combination of Evenhaim and Settimi would still permit the searching of a "predefined list" of patients to obtain the record for those patients.

15. Also, a POSA would have understood from Evenhaim's full disclosure that searching by original, unaltered patient names is not relevant to its goal. Specifically, Evenhaim explains that the "micro-level records" that it seeks to maintain for its rich dataset may be "identity-free micro-data." EX1005, 10:29-32,

12:36-52, Fig. 4 ("micro data"); *see also* EX1006, [0038], [0043]. Evenhaim also explains that its "parameter list may [] include specific individuals by name ***or ID or the like[]***." EX1005, 8:30-43 ("[T]he aggregator may accept a query that includes . . . a list of names or a combination of a few fields that together can allow for identification."). This makes clear to a POSA that records with, *e.g.*, original patient names, is not needed, so long as the search for the patient records can be accomplished by some "ID or the like[]." *Id*. As explained in my Prior Declaration, a "token" is simply a representation of data. EX1003, ¶¶ 29, 45, 75-76.

16. Thus, Settimi's database design would not harm Evenhaim's goals.

D. The Combination of Evenhaim and Settimi Would Not Violate HIPAA

17. Vigilytics asserts that using public keys for tokenization on both the aggregator side and data source side, in Evenhaim, would risk that a bad actor at the aggregator could reverse engineer patient identities corresponding to records returned from the data source. POR, 28-30. Specifically, Vigilytics hypothesizes that a bad actor at Evenhaim's aggregator, in using a key to encrypt (*e.g.*, tokenize) a patient's identifying information, could save the token and original name in, *e.g.*, a table to attempt to look for the same token in the returned search results to determine which patients correspond to the records.

18. I disagree that a POSA would view this as a problem for several reasons.

19. First, the ’012 Patent’s design would also be subject to the same type of attack inasmuch as the token generator 314 at the encryption server is not part of any closed off healthcare system (*i.e.*, source sites), as shown in Figure 3. EX1001, Fig. 3, 6:39-41, 8:25-42. Dr. Rubin acknowledged that a POSA would address this issue, to the extent it is a concern, using “known security techniques.” EX1014, 25:13-28:17. He also explained that a system design would seek to use a trusted party. EX1014, 52:2-53:17. I agree with his opinion in this regard and a POSA would have similarly employed known techniques to guard against attacks in implementing Evenhaim, Settimi, and combinations thereof. In fact, Evenhaim and Settimi are both directed to *achieving* HIPAA compliance. EX1014, 33:12-34:4; EX1005, 2:5-26. Also, both Evenhaim and Settimi describe using hash functions to de-identify records (*see* EX1005, 2:5-26; EX1006, [0038], [0041]), which the ’012 Patent itself uses to comply with HIPAA. HIPAA explicitly allows for hash functions to encrypt PII for de-identification. EX1016, 30-31.

20. Second, Evenhaim offers an option for protecting the encryption key. Evenhaim describes that tokenization may occur at the aggregator. EX1005, 12:24-34. To the extent that the designer is concerned about the aggregator having access to the key, Evenhaim explains that the key may be held at that site by an “escrow

agent." EX1005, 12:63-66; EX1014, 132:5-21. Dr. Rubin acknowledged that such an agent could hold keys for encryption and that agreements with parties could be used to ensure the parties maintain privacy. EX1014, 51:17-53:17, 29:13-30:10 ("So I think in that hypothetical scenario it would be either a contractual agreement or just an understanding that the point of this encryption server is that it should not be sharing all of its information with the public."); EX1005, 5:12-28. HIPAA also identifies business agreements to maintain privacy. EX1021 (defining business associate), EX1020, 3; EX1016, 6.

21. Third, HIPAA offers different ways to de-identify healthcare data in a compliant manner. One option is known as the expert determination method, which allows for de-identification through accepted statistical and scientific principles, which leave a small risk that the information could identify an individual. EX2006 (§ 164.514(b)(1)); EX1016, 12-13. Vulnerabilities can remain in even well-designed system; most countermeasures can be broken. The safe harbor is another option, which dictates the removal of specific identifying information to render the data no longer covered by HIPAA. *See* EX2006, (45 C.F.R. § 164.514(b)(2)); EX1016, 9-11 ("safe harbor"); EX1006, [0009]. This gives the POSA options for ensuring privacy through implementation designs. Whether implementing the design of the '012 Patent, Evenhaim, or Settimi, the POSA would ensure the system design is compliant. *See* EX1005, 3:17-31, 4:34-48, 5:46-6:10, 8:18-22,

14:7-13, 15:15-24, 14:59-67, 3:26-31, 5:20-22 (noting the "HIPAA Business Associate Agreement"); 12:61-66 (noting the concept of a "trusted third party"); Ex. 1006, [0017], [0027], [0039]-[0043].

22. Fourth, the idea of bad actors using, *e.g.*, a public key to encrypt a known identifier and then maintaining the identifier and encrypted version in correspondence to attempt to circumvent security measures has been a known manner of attack for some time. The attack is referred to by a POSA a "plain text" attack (*e.g.*, "chosen plain text" and "known plain text"). Long before the '012 Patent, it was known by those in the field that various defenses could be used against plain text attacks, if needed. One such defense is a "salt" incorporated into the encryption process (*e.g.*, incorporating random data) so as to make a lookup table difficult to use. EX1022, 5-6; EX1023, 597. Another defense uses cypher block chaining, which ties pieces of encrypted data together to make plaint text attacks impractical. Both techniques would have been known to a POSA for guarding against the hypothetical attack raise by Vigilytics.

23. Also, my Prior Declaration identified another way to guard against a plain text attack. EX1003, ¶ 42. Specifically, the centralized database could simply add another level of encryption to the token before returning search results. This concept of using multiple layers of encryption would also have been known to a

POSA before the ’012 Patent, and the concept is generally described in described U.S. Pat. No. 7,668,820. EX1024, 2:20-51, 5:26-61.

E. Evenhaim and Murphy Suggest Using Minimums

24. I understand that the POR asserts that Murphy does not teach claim element [7.g]—namely, “the healthcare information being produced based on a minimum number of matched tokens.” POR, 41-44; Pet., 26-27; EX1003, ¶¶ 88-90. That assertion ignores Evenhaim, which applies a requirement for a minimum number of individuals at the user side (query) and database side (search results) to safeguard patient identity. EX1005, 13:62-65, (user side: “a predetermined minimum number of individuals … into a ‘parameter list’”), 8:13-48 (user side: “large enough list”; “transmitting the parameter list may include transmitting a sufficiently large list”), 16:5-32 (database side: “The query engine determines whether the number of participants in each program and the % ***participants matched*** are above a level that ensures consumer individual privacy …. If not, the query engine responds with: group name ‘cannot be analyzed because of privacy safeguards.’”).

25. In any event, Murphy also suggests the use of a minimum, which a POSA would have understood could be implemented at either side of the process. Specifically, Murphy describes checks to ensure at least a minimum number of records were identified. EX1009, 553. If that minimum is not met, a message is

provided that says "<3." *Id.* As discussed in more detail below, for Ground 3, that does not answer the query posed (*e.g.*, stating the number of hits). *See* POR, 67-68 ("rather than returning an absolute value"). As also discussed below, Murphy is not limited to the nature of the query, such that a POSA would have understood the minimum would have been imposed regardless of the type of query (e.g., a query for specific patient records, as taught by Evenhaim). EX1009, 555 ("acceptable methods of obfuscation will be dependent on the types of data that need to be served back to the client application").

VI. GROUND 1: OBVIOUS (§ 103) OVER EVENHAIM AND MURPHY

26. I understand that Vigilytics tries to limit the encryption of the patient list described in Evenhaim to the general encryption that would be used for data transmission (*e.g.*, that there would be general encryption of the overall message). *See* POR, 20-23.

27. Evenhaim describes different manners/levels of encryption. In one portion, Evenhaim describes the encryption for general data transmission on which Vigilytics relies. EX1005, 13:28-43. Evenhaim also describes enhanced encryption for the patient list, which differs from general encryption for transmissions. *Id.*, 14:3-13. Evenhaim also states that ***parts of the parameter list*** may be encrypted. 1005, 8:43-48, 12:24-34 (explaining that encryption of an individual can happen anywhere in the system). A POSA would understand that this would suggest the

encryption of, for instance, particular fields in the patient list (*e.g.*, each individual name), and that such encryption may remain throughout the process, unlike general transmission encryption, which is decrypted by the party receiving the message.

28. In addition, as discussed above, Evenhaim describes that the list in the query can use an "ID" or the like (a token), instead of a name. EX1005, 8:30-43. Thus, a POSA would understand Evenhaim to suggest tokenization. As would have been appreciated by a POSA, tokenization had long been known and, in connection with patient names, it was known tokenization could be achieved using a combination of pieces of identifying information such as part of the person's name, the person's DOB, and part of the person's SSN. *See, e.g.*, EX1008, 5:2-19; *see also* EX1005, 13:1-12. This could be achieved by encrypting parts of the patient list, as Evenhaim describes. In fact, Evenhaim explains that its aggregator converts the user's query into a format that the database understands. EX1005, 8:30-56. Thus, Evenhaim's description of using an ID or the like (instead of a name) in the parameter list sent to the data sources (EX1005, 8:30-43) suggests tokenization, which has been defined simply as an ID (EX1003, ¶¶ 29, 45 (defining "token")).

VII. GROUND 3: OBVIOUS (§ 103) OVER DICK, LANDI, AND MURPHY

A. Prior Art References

i. Dick

29. Dick describes a repository of de-identified medical records that allows for querying of a group of individuals. EX1007, Abstract, [0024]. As discussed in my Prior Declaration, Dick meets the claim requirements for a search for a specific group of humans. EX1003, ¶ 216. While Dick acknowledges HIPAA restrictions and the benefits of de-identification, Dick generally "contemplates" "methods and processes" for the same. EX1007, [0046]. Dick does not detail specific technical operations for de-identification.

ii. Landi

30. Landi provides a more technical description of how a POSA could de-identify patient records using, in particular, encrypted IDs (*i.e.*, tokens). The tokens enable patient records to be located and released to third-party entities without revealing patient identities. Landi's system does permit the re-identification of the records, but only at the places, *i.e.*, covered entities, where the de-identification occurred. EX1008, 7:22-30. In that manner, Landi protects privacy.

B. A POSA Would Be Motivated to Combine Dick and Landi

31. I understand that Vigilytics argues that a POSA would not have been motivated to combine Dick and Landi because Dick already provides de-

identification methods. POR, 52-54. The paragraphs cited by Vigilytics (EX1007, [0045]-[0047]) merely discuss, in general, the requirements in the HIPAA rules (remove PII or statistical obfuscation) and there are different methods for doing so. *Compare* EX1007, [0045]-[0047] *with* EX2006 (45 C.F.R. § 164.514). Dick simply invites one to use de-identification "methods," without endorsing any one particular technical operation. EX1007, [0046].

32. This is consistent with my deposition testimony. EX2002, 79:17-81:2. Specifically, it is true that a POSA would be able to de-identify without going beyond Dick. However, one such method is explained in Landi. A POSA would have understood that any method could have been selected, with Landi's tokenization being a preferred option.

C. A POSA Would Not Understand Landi's Design to Violate HIPAA

33. I disagree with Vigilytics' assertion that Landi's design violates HIPAA. POR, 59-60. Landi explicitly states that its design presents "no HIPAA issues" and that its goal is HIPAA compliance. EX1008, 3:52-57, 8:38-55. A POSA would have no reason to doubt Landi's statement in this regard, and, given Vigilytics' heightened POSA standard, the POSA certainly would have been more than capable of implementing Landi in a HIPAA compliant manner.

34. Also, I note that Vigilytics cites my deposition testimony to suggest that produced healthcare information in Dick and Landi is not absent PII. POR, 65-66. The cited testimony indicates that, in Landi's design, the returned search results may include the encrypted ID. EX2002, 93:23-94:7. As Landi explains, only the original encrypting entities can de-identify the information. EX1008, 5:20-31, 6:61-65, 7:20-30, 10:32-45, 11:13-17, 1:14-22. Thus, Landi suggested protecting PII and a POSA would implement Landi to do just that to comply with HIPAA.

D. The Application of Murphy

35. As discussed above, Murphy is directed to preventing the production of protected information in connection with instances in which too few records would be returned, leading to possible identification of a patient. Consequently, Murphy describes performing a check to ensure at least a minimum number of records were identified. EX1009, 553, 555. If the minimum number is not met (*e.g.*, 3), in the example, a message indicates that the number of hits is, *e.g.*, "<3." *Id.* Where the query was for the number of patients having a specific diagnosis, the message does not answer the query.

i. Murphy Does Not Provide an Answer When the Minimum Threshold is not Met

36. I understand that Vigilytics asserts that because Murphy's system "returns a numerical result" it must be understood that "the query is still answered." POR, 67-68. I disagree. Because, in the example in Murphy, the

question asks for the precise number of patients with, *e.g.*, a particular condition, the user does not receive the answer to that question if the answer would be below the threshold. EX1009, 555. In that manner, the "<3" answer acts as an error message to the user.

ii. Murphy's Teaching is Not Limited to One Type of Query

37. I understand that Vigilytics suggests that Murphy is limited to one type of query. POR, 17, 64, 67-68. Of note, regardless of the example query discussed in Murphy, the ground relies upon Dick and Landi to establish that it was known to query databases to find records for specific groups of individuals, as discussed above. Murphy is relied upon simply to teach that, for privacy reasons, a POSA would understand that a system would preferably set a minimum number of patients to guard against allowing the user to match a particular patient to the related healthcare information at issue. EX1009, 552-53. That concept is applicable regardless of the nature of the query. Specifically, Murphy explains that its operation can be used for various types of queries. EX1009, 556 ("does not limit the logic of the query").

38. Also, a POSA would understand Murphy to be generally about preventing the return of too few hits, which could allow a user to identify sensitive medical information for a particular patient. EX1009, 552 ("An attack on the system would occur by someone entering criteria into the query tool that would

result in only one matching person."), 553 ("attempts to discern individuals"). A POSA would understand that the precise point of the blockage is simply a design choice, as Murphy's stated concern is a user trying to identify one individual through narrowing parameters. EX1009, 552-53. Murphy's goal is to prevent narrow parameters that would allow for a privacy violation, regardless of the type of query or manner of attack by the user (*e.g.*, narrow queries, narrow hits, etc.).

VIII. CONCLUSION

39. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

February 26, 2025

Paul C. Clark DSc.