

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

DECLARATION OF AVIEL D. RUBIN
IN SUPPORT OF PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	BACKGROUND	5
	A. Introduction	5
	B. Experience and Qualifications.....	5
	C. Topics of Opinions	11
	D. Materials Considered.....	13
II.	My Understanding of the Law.....	15
	A. Claim construction.....	15
	B. Priority	16
	C. Anticipation	16
	D. Inherency	16
	E. Obviousness.....	17
III.	THE '641 PATENT	19
IV.	HIPAA Background	33
	A. Privacy Rule	33
	B. Security Rule	35
V.	LEVEL OF ORDINARY SKILL IN THE ART	35
VI.	CLAIM CONSTRUCTION.....	37
VII.	THE GROUNDS FOR UNPATENTABILITY	37
VIII.	THE PRIOR ART.....	38
	A. Overview of the Evenhaim Reference (EX1005)	38
	B. Overview of the Settimi Reference (EX1006)	41
	C. Overview of the Dick Reference (EX1007)	42

D. Overview of the Landi Reference (EX1008)	45
E. Overview of the Murphy Reference (EX1009).....	49
IX. THE CHALLENGED CLAIMS ARE NOT UNPATENTABLE	51
A. Analysis of Ground 1: the Evenhaim Reference Fails to Render Claims 1–19 Obvious.....	51
1. Evenhaim’s data aggregator does not produce a token for each individual included in a group composed of multiple individuals identified in a request	52
2. Evenhaim’s data aggregator does not convey request tokens for individual patients to data source entities	61
3. Evenhaim’s data source entities do not perform the alleged “token matching” to search de-identified healthcare data	67
4. Evenhaim fails to disclose or render obvious multiple limitations of independent claims 1, 7 and 14	73
B. Analysis of Ground 2: the Evenhaim-Settimi Combination Fails to Render Claims 1–19 Obvious.....	75
1. The Evenhaim-Settimi combination fails to disclose or render obvious multiple limitations of independent claims 1, 7 and 14	77
2. The Evenhaim-Settimi combination would not have been obvious because integration of Settimi’s teachings would have violated Evenhaim’s express preference for searching original, micro-level patient data	79
C. Analysis of Ground 3: the Dick-Landi Combination Fails to Render the Challenged Claims Obvious.....	81
1. The Petition fails to show that a POSITA would have combined Dick and Landi in a manner that would lead to the claimed invention	81
2. The Dick-Landi combination does not disclose or render obvious elements [1.b]-[1.c], [7.a]-[7.b], or [14.c]-[14.d]: an encryption server for producing a token for each individual included in a group identified in a request for healthcare information	84
3. The Dick-Landi combination does not disclose or render obvious elements [1.f], [7.e]-[7.f], [14.f]: identifying tokens in a set of de-	

identified healthcare data that correspond to request tokens for
individuals in a group.....91

4. The Dick-Landi combination does not disclose or render obvious
elements [1.h], [7.h], [14.h]: the produced healthcare information is
absent personally identifiable information.....94

5. Landi’s method of de-identification does not satisfy HIPAA
requirements 94

D. Analysis of Ground 4: the Dick-Landi-Murphy Combination Fails to
Render the Challenged Claims Obvious 113

1. Analysis 113

X. CONCLUSION 117

I, Aviel D. Rubin, Ph.D., declare as follows:

I. BACKGROUND

A. Introduction

1. I have been retained by counsel for Vigilytics LLC (Patent Owner) as a technical expert for the *Inter Partes* Review (IPR) proceeding identified above. I submit this declaration to offer my opinions on the patentability of claims 1–19 of U.S. Patent No. 9,118,641 (“the ’641 Patent”).

2. As I will discuss in more detail in the sections that follow, it is my opinion that claims 1–19 are patentable and non-obvious even in view of the Petitioner’s cited references.

3. I am not and never have been, an employee of Vigilytics. I received no compensation for this declaration beyond my normal hourly compensation based on my time actually spent analyzing the ’641 patent, the prior art publications cited below, and issues related thereto, and I will not receive any added compensation based on the outcome of any IPR or other proceeding involving the ’641 patent.

B. Experience and Qualifications

4. I am over the age of 18 and am competent to write this declaration. I have personal knowledge or have developed knowledge of these technologies based upon education, training, or experience, of the matters set forth herein.

5. I have more than 30 years of experience in the field of computer

science, and specifically, computer security, with my latest research focus being on security for healthcare IT systems. A copy of my curriculum vitae is attached as Appendix A hereto.

6. I received my Ph.D. in Computer Science and Engineering from the University of Michigan, Ann Arbor in 1994, with a specialty in computer security and cryptographic protocols. My thesis was titled “Nonmonotonic Cryptographic Protocols” and concerned authentication in long-running networking operations.

7. I am a Professor Emeritus in Computer Science at Johns Hopkins University (the “University”). I joined the Computer Science faculty at the University in 2003 and was promoted to full professor with tenure in April 2004. As a member of the faculty, I perform research, teach graduate and undergraduate courses in computer science and related subjects, advise undergraduate and Masters students, and supervise the research of Ph.D. candidates and other students. I have taught courses including Networking, Security and Privacy in Computing, Cryptography, and Advanced Topics in Computer Security. In September 2023, I was appointed Professor Emeritus.

8. I also served as the Technical Director of the University’s Information Security Institute (“ISI”). The ISI is the University’s focal point for research and education in information security, assurance, and privacy. The University, through the ISI’s leadership, has been designated as a Center of Academic Excellence in

Information Assurance by the National Security Agency and leading experts in the field.

9. I also have significant industry experience. Since 2011, I have served as the founder and chief scientist of Harbor Labs, a software and networking consulting firm specializing in data security and privacy. Previously, from 2005 to 2011, I served as the founder and President of Independent Security Evaluators (“ISE”), a computer security consulting firm. In that capacity, I guided ISE through the qualification process to become an independent testing laboratory for Consumer Union, which produces the Consumer Reports magazine. ISE provided consulting services to various companies on potential security flaws and weaknesses in products and systems. These companies included Fortify Software, Verdasys, and Security First Corp. As an independent testing laboratory for Consumer Union, I managed an annual project where we tested popular anti-virus products. Our results were published in Consumer Reports each year for three consecutive years.

10. After receiving my Ph.D., I began working at Bellcore in its Cryptography and Network Security Research Group from 1994 to 1996. During this period, I focused my work on computer security. While at Bellcore, I published an article titled “Blocking Java Applets at the Firewall” about the security challenges of dealing with JAVA applets and firewalls, and a system that

we built to overcome those challenges.

11. In 1997, I moved to AT&T Labs, Secure Systems Research Department, where I continued to focus on computer security. From 1995 through 1999, in addition to my work in industry, I served as Adjunct Professor at New York University, where I taught undergraduate classes on computer, network and Internet security issues.

12. I stayed in my position at AT&T until 2003, when I left to accept a full time academic position at Johns Hopkins University . The University promoted me to full professor with tenure in April 2004.

13. I serve, or have served, on several technical and editorial advisory boards. For example, I served on the Editorial and Advisory Board for the International Journal of Information and Computer Security. I also served on the Editorial Board for the Journal of Privacy Technology. In addition, I have been Associate Editor of the IEEE Security and Privacy Magazine and served as Associate Editor of the Association for Computing Machinery's ("ACM") Transactions on Internet Technology. I also served as Associate Editor of the journal Communications of the ACM, and I was an Advisory Board Member of Springer's Information Security and Cryptography Book Series. I also have served in the past as a member of the Defense Advanced Research Projects Agency's Information Science and Technology Study Group, a member of the Government

Infosec Science and Technology Study Group of Malicious Code, a member of the AT&T Intellectual Property Review Team, Associate Editor of the Electronic Commerce Research Journal, Co-editor of the Electronic Newsletter of the IEEE Technical Committee on Security and Privacy, a member of the board of directors of the USENIX Association (the leading academic computing systems society), and a member of the editorial board of the Bellcore Security Update Newsletter.

14. I have spoken on information security and electronic privacy issues at more than 50 seminars and symposia. For example, I presented keynote addresses on the topics “Security of Electronic Voting” to Computer Security 2004 Mexico in Mexico City, Mexico, in May 2004; “Electronic Voting” to the Secure Trusted Systems Consortium 5th Annual Symposium in Washington, D.C., in December 2003; “Security Problems on the Web” to the AT&T EUA Customer Conference in March 2000; and “Security on the Internet” to the AT&T Security Workshop in June 1997. I also presented a talk about hacking devices at the TEDx conference in October 2011 and another TEDx talk on the same topic in September 2015.

15. I am a named inventor on ten United States patents, all in the information security area. The patent numbers and titles as well as my co-inventors are listed on the attached curriculum vitae. In March 2004, I was asked by the Federal Trade Commission to submit a report commenting on the viability and usefulness of a national do not email registry. I Request for Information on

Establishing a National Do Not E-mail Registry” on May 10, 2004.

16. I have also testified before Congress regarding the security issues with electronic voting machines and in the United States Senate on the issue of censorship. I also testified in Congress on November 19, 2013, about security issues related to the government’s Healthcare.gov website.

17. I am the author or co-author of five books regarding information security issues: Brave New Ballot, Random House, 2006; Firewalls and Internet Security (second edition), Addison Wesley, 2003; White-Hat Security Arsenal, Addison Wesley, 2001; Peer-to-Peer, O’Reilly, 2001; and Web Security Sourcebook, John Wiley & Sons, 1997. I am also the author of numerous journal and conference publications.

18. I was the founding director of the Health and Medical Security lab at Johns Hopkins. In addition to our research into health information security, we had an educational program that focused on teaching healthcare IT professionals about the HIPAA privacy and security rules. In addition, I am the founder of Harbor Labs, which focuses on medical device security, and we often refer to the HIPAA rules as part of our security work for our clients.

19. Additional details of my education and employment history, recent professional service, patents, publications, and other testimony are set forth in my current curriculum vitae, attached to this declaration as Appendix A.

20. As is apparent from the above description, virtually my entire professional career has been dedicated to issues relating to computer networks, particularly with respect to security.

21. I am being compensated \$925 per hour for my time spent working in connection with this case. My compensation is in no way related to the outcome of this litigation. If called as a witness, I would testify as to the statements and opinions contained in this report.

22. I am not a legal expert and offer no opinions on the law. However, I have been informed by counsel of the various legal standards that apply, and I have applied those standards in arriving at my conclusions.

C. Topics of Opinions

23. I have been asked to render, and I provide in this declaration, an opinion regarding whether the references presented in the Petition and discussed in the declaration of Dr. Paul Clark disclose or render obvious claims 1–19 of U.S. Pat No. 9,118,641 (“the ’641 patent”).

24. In my opinion, the Petition has not shown that claims 1–19 are unpatentable as obvious in view of Evenhaim, whether taken alone or in combination with Settini. Likewise, the Petition has not shown that claims 7–10 and 13 are unpatentable as obvious in view of the Dick-Landi combination; and the Petition has not shown that claims 1–6, 11–21, and 14–19 are unpatentable as

obvious in view of the Dick-Landi-Murphy combination.

25. For example, in Ground 1, the Petition mischaracterizes key aspects of Evenhaim's disclosure. Among other things, the Petition conflates Evenhaim's separate encryptions for data transmission security and data mergers to conjure an embodiment in which data source entities allegedly search de-identified patient data by matching encrypted request tokens to corresponding tokens associated with the de-identified data. But these features are never disclosed in Evenhaim and Evenhaim's system would never operate as Petitioner contends. The Petition's interpretation of Evenhaim is both contradicted by portions of the reference not acknowledged in the Petition and is inconsistent with Evenhaim's express teaching against searching on de-identified or agglomerated data, as would be required by Petitioner's theory. Likewise, Ground 2 based on Evenhaim in view of Settimi suffers from these same defects as Ground 1, along with additional problems as described in this Declaration.

26. In Ground 3, the Petition fails to demonstrate a motivation to combine Dick and Landi. Even if combined, the resulting system would not achieve multiple limitations recited in the Challenged Claims. The combination, for example, would entirely lack an encryption server that produces a token for each individual included in a group composed of multiple individuals identified in a request for healthcare information.

27. And Ground 4 adds Murphy to the Dick-Landi combination but inherits the same defects from Ground 3. The Petition's reliance on Murphy is also non-availing as Murphy does not block queries as assumed in the Petition.

28. For each of these and the additional reasons described in detail in this Response, the Petition fails to show that any of the Challenged Claims would have been obvious. Grounds 1–4 should accordingly be dismissed and the patentability of the claims confirmed.

D. Materials Considered

29. In preparing this Declaration I have relied on my education, training, and experience. I have also considered the following materials:

Paper No.	Description
1	Petition for <i>Inter Partes</i> Review of U.S. Patent No. 9,118,641

Exhibit No.	Description
1001	U.S. Patent No. 9,118,641
1002	File History of U.S. Patent No. 9,118,641
1003	Declaration of Dr. Paul Clark
1004	Curriculum Vitae Of Dr. Paul Clark
1005	U.S. Pat. No. 7,823,207 (“Evenhaim”)

Exhibit No.	Description
1006	U.S. Pat. Appl. Publ. No. 2007/0294111 (“Settimi”)
1007	U.S. Pat. Appl. Publ. No. US 2002/0111833 (“Dick”)
1008	U.S. Pat. No. 7,519,591 (“Landi”)
1009	Shawn N. Murphy and Henry C. Chueh, <i>A Security Architecture for Query Tools used to Access Large Biomedical Databases</i> , 2002 AMIA Annual Symposium Proceedings, 552 (2002) (“Murphy”)
1010	<i>Milliman, Inc. v. Gradient A.I. Corp.</i> , No. 1:21-Cv-10865-NMG (D. Mass.), Dkt. 108.
1011	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, <i>Kerberos: An Authentication Service for Open Network Systems</i> , Winter 1988 Usenix Conference (1988).
2002	IPR2024-00226, Deposition Transcript of Dr. Paul Clark, dated 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

Exhibit No.	Description
	disclosures of protected health information)
2007	45 C.F.R. §75.2 (Definitions)

II. MY UNDERSTANDING OF THE LAW

30. I am not a lawyer and do not provide any legal opinions. Although I am not a lawyer, I have been advised that the following legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

A. Claim construction

31. I understand that, for purposes of my analysis in this IPR, the terms appearing in the patent claims should be interpreted according to their “ordinary and customary meaning.” In determining the ordinary and custom meaning, I understand that the words of a claim are first given the plain meaning that those words would have had to a person of ordinary skill in the art (“POSITA”) at the time of the claimed invention. I also understand that the structure of the claims, the specification, and file history also may be used to better construe a claim insofar as the plain meaning of the claims cannot be understood. Moreover, I understand that even treatises and dictionaries may be used, albeit under limited circumstances, to determine the meaning attributed by a POSITA to a claim term at

the time of filing. I also understand that the words of the claims should be interpreted as they would have been interpreted by a POSITA at the time the alleged invention was made (not today). I have followed these guidelines in my analysis.

B. Priority

32. I understand that a continuation application is a later-filed application that has the same disclosure (specification and figures) as an earlier filed application to which the later-filed application claims priority. A continuation is generally entitled to the same priority date as the later-filed application to which it claims priority.

C. Anticipation

33. I understand that a claim can be invalid based on anticipation if each limitation of the claim is found in a single prior art reference (including any incorporated material), either expressly or inherently.

D. Inherency

34. I understand that a prior art reference inherently discloses subject matter that is not expressly disclosed, but nonetheless necessarily flows from the disclosure. However, the fact that a certain result or characteristic may be present in the prior art reference is not sufficient to establish inherency. Accordingly, a certain result or characteristic is not inherently disclosed if there is a single potential alternative for what a reference necessarily discloses.

E. Obviousness

35. I understand that a patent claim is invalid if the claimed invention would have been obvious to a POSITA at the time of the purported invention, which is often considered the time the application was filed. Thus, even if all of the claim limitations are not found in a single prior art reference that anticipates the claim, the claim can still be invalid.

36. To obtain a patent, a claimed invention must have, as of the priority date, been nonobvious in view of the prior art in the field. I understand that an invention is obvious when the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art.

37. I understand that a conclusion of obviousness may be based upon a combination of prior art references. However, I also understand that a patent composed of several elements may not be proved obvious merely by demonstrating that each of its elements was independently known in the art; rather, there must be an appropriate articulation of a reason to combine the elements from the prior art in the manner claimed. Such reasons include the following:

38. combining prior art elements according to known methods to yield predictable results;

39. simple substitution of one known element for another to obtain predictable results;
40. use of a known technique to improve similar devices (methods or products) in the same way;
41. applying a known technique to a known device (method or product) ready for improvement to yield predictable results;
42. “obvious to try” – choosing from a finite number of identified, predictable solutions with a reasonable expectation of success;
43. known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; and
44. some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art teachings to arrive at the claimed invention.
45. I also understand that certain objective indicia can be important evidence regarding whether a patent is obvious or nonobvious. Such indicia include:
46. commercial success of products covered by the patent claims;
47. a long-felt need for the invention;

- 48. failed attempts by others to make the invention;
- 49. copying of the invention by others in the field;
- 50. unexpected results achieved by the invention as compared to the closest prior art;
- 51. praise of the invention by the infringer or others in the field;
- 52. the taking of licenses under the patent by others;
- 53. expressions of surprise by experts and those skilled in the art at the making of the invention; and
- 54. the patentee proceeded contrary to the accepted wisdom of the prior art.
- 55. To the extent these factors have been brought to my attention, I have taken them into consideration in rendering my opinions and conclusions.

III. THE '641 PATENT

56. The '641 Patent explains that health insurers previously lacked sufficient access to protected health information ("PHI") stored by health providers, such as pharmacies, for individuals in small and midsize groups (e.g., groups of 10–1000 individuals). EX1001, 1:14–36. PHI for members in these groups, such as an individual, e.g., "Jack," and his dependents, could be used by health insurers to better understand, assess the risk, and appropriately price premiums for the associated future cost of providing health insurance to the group.

EX1001, 4:4–24. The PHI for Jack was previously insufficiently accessible because, as the '641 Patent explains, Federal laws, such as the Health Insurance Portability and Accountability Act (“HIPAA”), prohibit source sites that possess Jack’s PHI from releasing it to third parties without Jack’s permission. Under HIPAA, the source sites can release only irreversibly de-identified data without Jack’s (or another patient’s) permission. EX1001, 3:65–4:3. PHI can include “[d]ata that associates patient identity with health information” *Id.* at 1:26–28.

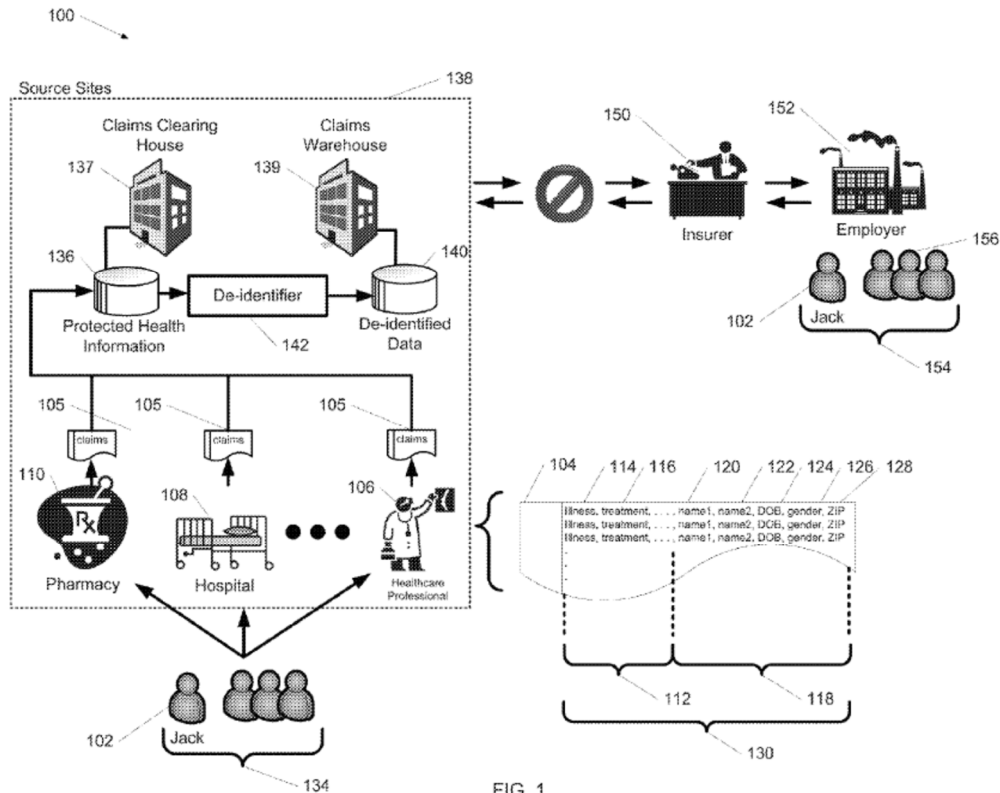


FIG. 1

'641 Patent, FIG. 1

57. As shown in FIG. 1 above, a “health insurer 150, for example, may be interested in the medical history information contained in Jack’s PHI 130. Jack’s

employer 152 may like to buy a group health insurance policy for the group 154 made up of Jack 102 and his coworkers 156. If the group 154 is too small, the insurance company 150 may be unwilling or unable to share medical claims history with the group 154 that would allow for an assessment of the potential risk from future medical claims for the group 154. The insurer 150 would also like to use the medical history from the group 154 to assess the risk of claims and set the group health insurance premium appropriately. Unfortunately, the group 154 may also be too large for the insurance company 150 to practically obtain permission from each person in the group, without which HIPAA prohibits the healthcare providers 138 from releasing the PHI 136 to the insurer 150. The de-identified data 140, which the healthcare providers or other source sites 138 could release without permission, is not useful to the insurer 150 because the insurer has no way to know whether it corresponds to the people in the group 154. With no way to obtain medical history data for the group, the insurer 150 cannot set the group insurance premium acceptably.” EX1001, 4:4–24.

58. To address this conundrum, the '641 Patent disclose novel methods and systems to implement specific token generation and anonymization approaches to achieve a new computer capability: systems able, in response to a request for information regarding a group of individuals who have not authorized PHI disclosure, to provide to third parties (e.g., insurance companies or professional

employer organizations, known as “PEOs”) irreversibly de-identified healthcare information from which the third party may calculate a risk score used in setting an insurance premium for the group, while complying with federal privacy regulations, including HIPAA.¹ *See, e.g., id.* at 4:25–30. This was a significant advancement because prior to the invention, signed authorizations had to be collected from individuals in the request, which was an impediment to a viable product. Although tokenized health data had been used for other purposes prior to the ’641 Patent, it had not been used in the particular context or manner described in the ’641 Patent. *Id.* FIG.3 illustrates an example system implemented in accordance with the novel solutions described in the ’641 Patent:

¹ Importantly, the irreversibly de-identified healthcare information for individuals must only be released to a third party that does not have access to the personally identifying information (PII) used to generate the request. Otherwise, the third-party might match PII from the request to the de-identified data patient-level data to uncover the patient’s identify. 45 C.F.R §164.514 (a),(c)

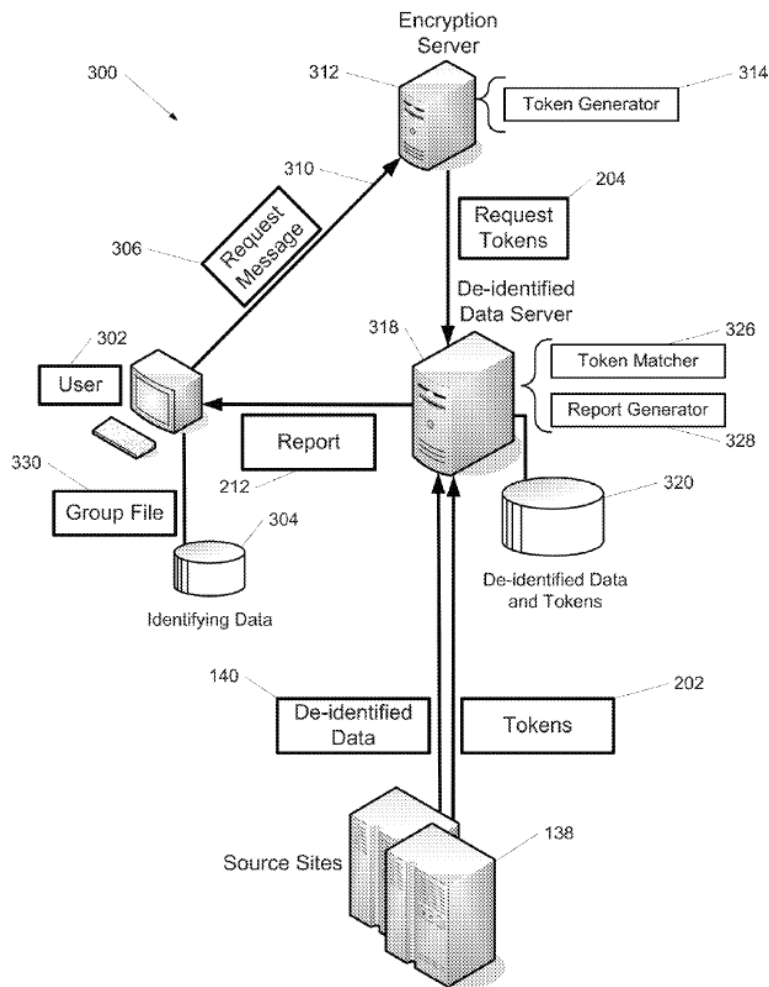


FIG. 3

59. As shown in FIG. 3, a user, e.g., an insurer, requests de-identified data that characterizes a group of identified individuals, where the de-identified data may reflect information regarding medical claims, hospital claims, and prescription history (such as the drug categories and drug indications associated with the drugs in the de-identified data). EX1001, 6:6–8, 6:59–62. In this example, the insurer can send a request to a third party. *Id.*, 4:32–33. The request “uniquely identifies” each individual in the group, which could be a group of individuals for which

health insurance is sought. *Id.*, 5:12–30. The third party, for example using an “encryption server,” generates a “request token” for each individual in the group based on the personally identifiable information for each individual in the group. *Id.*, 4:32–35, 5:35–38. The encryption server can generate the request token such that the request token is similarly encrypted to the token associated with the information to be produced. *Id.*, 2:16–18. For example, the encryption server may use the same token generator as used to generate the tokens for the de-identified data or it may use any other means that generates a comparable token for the same personally identifiable information. *Id.*, 5:44–67.

60. The identities of the individuals are unattainable from the tokens implemented according to the ’641 Patent. *Id.*, 4:30–32 (tokens “correspond to persons treated by healthcare providers but do not reveal the identities of the treated individuals”). That way, the tokens are reproducibly irreversible. *Id.*, 4:29–30 (system “associates unique tokens 202 with irreversibly de-identified data 140”), 6:8–12 (the de-identified data is processed “in a way that leaves it irreversibly de-identified”). In that connection, the tokens are generated from personally identifiable information of the individuals using “one or more encryption techniques” such as a hash function. *Id.*, 5:54–67.

61. In one configuration, the encryption server sends generated request tokens to the data aggregator, or de-identified data server, that stores the de-

identified healthcare data. *Id.*, 4:35–37, 5:44–49. The data aggregator (or de-identified data server) stores irreversibly de-identified healthcare data for many individuals. The de-identified healthcare data can comprise data from source sites such as pharmacies, healthcare professionals and electronic claim clearing houses. *Id.*, 5:45–49. The tokens are associated with the de-identified healthcare data of individuals. The data server, with a token matcher, can find all tokens in the de-identified healthcare data that match the request tokens from the encryption server. *Id.*, 4:37–41, 6:1–4. The de-identified healthcare data for the matched tokens can then be processed in a way that leaves it irreversibly de-identified, yet useful for an underwriting assessment of the group. *Id.*, 4:37–45, 6:8–15. The aggregator can retrieve the requested de-identified data for each of the individuals in the group, and the aggregator can provide the de-identified data associated with the group of individuals, without revealing the protected health information of the individuals in the group and without obtaining any authorization from the individual members of the group. This de-identified data can be included in a report provided to the user after tokens in the request are matched to tokens in the de-identified data. *Id.*, 6:62–67, 8:17–27, 8:27–31, 8:41–43. The recipient of the report, e.g., the insurer which has personally identifiable information about the individuals in the group does not have access to data associated with specific individuals. *Id.*, 4:51–54. “These features of the system maintain the privacy of the protected health

information.” *Id.*, 4:59–61 (reference numbers omitted).

62. The ’641 Patent explains that the above-described process may not be performed unless the request includes a minimum number of individuals. The minimum number (e.g., 10) is “chosen to make it effectively impossible to associate individual group members with individual tokens in the batch of request tokens” *Id.*, 5:40–43, FIGS. 2–3, 5–6.

63. For my analysis, I am adopting the claims indexing that the Petition uses, for consistency:

Index	Claim Term
1.a	A computer-implemented method comprising: receiving a request for healthcare information that characterizes a group composed of multiple individuals, the healthcare information being assembled from healthcare data that comprises de-identified information;
1.b	producing, by a processor of an encryption server, tokens,
1.c	wherein the identity of the individuals in the group is unattainable from the tokens, each token being associated with an individual in the group, each token being associated with a corresponding token in a set of de-identified healthcare data, and
1.d	each token in the set of de-identified healthcare data being associated with healthcare data for a corresponding individual;

1.e	when the group includes at least a minimum number of individuals,
1.f	producing the requested healthcare information that characterizes the group by identifying the tokens in the set of de-identified healthcare data and the associated de-identified healthcare data that correspond to the produced tokens,
1.g	wherein the produced tokens and the tokens in the set of de-identified data are similarly encrypted, and
1.h	the produced healthcare information is absent personally identifiable information and
1.i	has been produced without the individuals in the group having authorized production of such healthcare information that characterizes the group; and
1.j	providing the produced healthcare information to report the characteristics of the group composed of multiple individuals absent authorization at any time from the individuals in the group of individuals to provide the requested healthcare information.
2	The computer-implemented method of claim 1, wherein the healthcare information provided absent authorization from the group of individuals at any time is in conformity with the Health Insurance Portability and Accountability Act (HIPAA).

3	The computer-implemented method of claim 1, wherein receiving a request for healthcare information that characterizes a group of individuals from healthcare data includes receiving personally identifiable information associated with members of the group of individuals.
4	The computer-implemented method of claim 1, in which producing the requested healthcare information includes encrypting respective data that identifies each individual.
5	The computer-implemented method of claim 1, in which producing the requested healthcare information includes identifying at least a minimum number of corresponding tokens.
6	The computer-implemented method of claim 1, in which the healthcare data represents medical related information associated with the individuals of the group.
7.a	A system comprising: an encryption server, having a processor and a memory,
7.b	for producing a token for each individual included in a group composed of multiple individuals identified in a request for healthcare information that characterizes the group,
7.c	wherein the identity of the individuals in the group is unattainable from

	the tokens, each token being associated with a corresponding token in a set of de-identified healthcare data,
7.d	and each token in the set of de-identified healthcare data being associated with healthcare data for a corresponding individual;
7.e	a data server for producing the requested healthcare information that characterizes the group
7.f	by identifying the tokens in the set of de-identified healthcare data and the associated de-identified healthcare data that correspond to the produced tokens,
7.g	wherein the produced tokens and the tokens in the set of de-identified data are similarly encrypted,
7.h	and the produced healthcare information is absent personally identifiable information
7.i	and has been produced without the individuals in the group having authorized production of such healthcare information that characterizes the group; and
7.j	providing the produced healthcare information to report the characteristics of the group composed of multiple individuals
7.k	absent authorization at any time from the individuals in the group of

	individuals to provide the requested healthcare information.
8	The system of claim 7, wherein the healthcare information provided absent authorization from the group of individuals at any time is in conformity with the Health Insurance Portability and Accountability Act (HIPAA).
9	The system of claim 7, wherein the request for healthcare information that characterizes a group of individuals from healthcare data includes personally identifiable information associated with members of the group of individuals.
10	The system of claim 7, in which producing the requested healthcare information includes encrypting respective data that identifies each individual.
11	The system of claim 7, in which producing the requested healthcare information includes identifying at least a minimum number of corresponding tokens.
12	The system of claim 7, in which producing the requested healthcare information includes determining if the group includes at least a minimum number of individuals.
13	The system of claim 7, in which the healthcare data represents medical related information associated with the individuals of the group.

14.a	One or more computer readable storage devices storing instructions that are executable by a processing device, and upon such execution cause the processing device to perform operations comprising:
14.b	receiving a request for healthcare information that characterizes a group composed of multiple individuals, the healthcare information being assembled from healthcare data that comprises de-identified information;
14.c	producing, by a processor of an encryption server, tokens,
14.d	wherein the identity of the individuals in the group is unattainable from the tokens, each token being associated with an individual in the group, each token being associated with a corresponding token in a set of de-identified healthcare data, and each token in the set of de-identified healthcare data being associated with healthcare data for a corresponding individual;
14.e	when the group includes at least a minimum number of individuals,
14.f	producing the requested healthcare information that characterizes the group by identifying the tokens in the set of de-identified healthcare data and the associated de-identified healthcare data that correspond to the produced tokens,
14.g	wherein the produced tokens and the tokens in the set of de-identified

	data are similarly encrypted, and
14.h	the produced healthcare information is absent personally identifiable information and has been produced without the individuals in the group having authorized production of such healthcare information that characterizes the group; and
14.i	providing the produced healthcare information to report the characteristics of the group composed of multiple individuals absent authorization at any time from the individuals in the group of individuals to provide the requested healthcare information.
15	The computer readable storage devices of claim 14, wherein the healthcare information provided absent authorization from the group of individuals at any time is in conformity with the Health Insurance Portability and Accountability Act (HIPAA).
16	The computer readable storage devices of claim 14, wherein the request for healthcare information that characterizes a group of individuals from healthcare data includes personally identifiable information associated with members of the group of individuals.
17	The computer readable storage devices of claim 14, in which producing the requested healthcare information includes encrypting respective data that identifies each individual.

18	The computer readable storage devices of claim 14, in which producing the requested healthcare information includes identifying at least a minimum number of corresponding tokens.
19	The computer readable storage devices of claim 14, in which the healthcare data represents medical related information associated with the individuals of the group.

IV. HIPAA BACKGROUND

64. As noted above, the technology described and claimed in the '641 Patent allows entities such as insurance carriers to obtain reports that characterize de-identified health care data for a specific group of individuals while still complying with patient privacy laws such as HIPAA. *Supra*, §III. While the inventive technology is not limited to systems and methods that operate within the constraints of HIPAA, HIPAA nonetheless features prominently in examples described in the specification of the '641 Patent, the prior art applied in the Petition, and the obviousness analyses of the Petitioner and its witness (Dr. Clark). I therefore review particular aspects of HIPAA relevant to the parties' dispute.

A. Privacy Rule

65. The "HIPAA Privacy Rule" is a rule issued by the Department of Health and Human Services (HHS) under HIPAA. According to the HHS website,

the HIPAA Privacy Rule “address[es] the use and disclosure of individuals’ health information—called ‘*protected health information*’ by ‘*covered entities*’—or organizations that are subject to the Privacy Rule,” as well as standards for individuals’ privacy rights to understand and control how their health information is used.² EX2003, 3³.

66. The HIPAA Privacy Rule does not include any restrictions on the use or disclosure of *de-identified* health information. EX2003, 3; EX1008, 2:5–18; EX1005, 2:5–57. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. *Id.*

67. While not using the term “HIPAA Privacy Rule,” the ’641 Patent refers to it. For example, the ’641 Patent states that “Federal privacy laws . . . prevent insurance companies from obtaining protected health information without individual authorizations from [] each person in the group” and that HIPAA prohibits source sites that process a person’s PHI from releasing to third parties the person’s PHI without the person’s permission. EX1001, 1:33–36, 3:65–4:2.

68. The ’641 Patent also explains that the source sites can release only irreversible de-identified data without the person’s permission. *Id.*, 4:2–3. This is

² All emphasis added unless indicated otherwise.

³ All page numbers indicate the PDF page number unless indicated otherwise.

how the systems described in the '641 Patent can comply with HIPAA; by using de-identified healthcare data so that authorizations from the individuals in a request group are not required.

B. Security Rule

69. The HIPAA Security Rule specifically focuses on the protection of electronic protected health information (ePHI). EX2004, 2. It requires covered entities to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. EX2004, 6. These safeguards include access control, audit controls, and policies for handling security incidents. EX2004, 8–9.

70. An important difference between the Privacy Rule and Security Rule is that the Privacy Rule covers all forms of PHI (electronic, paper, and oral) while the Security Rule focuses more narrowly on ePHI and ensuring that electronic systems and processes used to handle this information are secure against breaches and unauthorized access. EX2004, 5, 9–10.

V. LEVEL OF ORDINARY SKILL IN THE ART

71. I have been informed and understand that the question of whether patent claims would have been novel and non-obvious over the prior art is assessed from the perspective of a person of ordinary skill in the art (“POSITA” or “POSA”). Counsel has advised me that, to determine the appropriate level of skill

of a POSITA, I may consider the following factors: (a) the types of problems encountered by those working in the field and prior art solutions thereto; (b) the sophistication of the technology in question, and the rapidity with which innovations occur in the field; (c) the educational level of active workers in the field; and (d) the educational level of the inventor. I have considered those factors and also considered the computer scientists, professors, researchers and students that I worked with over my career, including at Johns Hopkins University.

72. I understand the Petition contends that a POSITA “would have a Bachelor of Science degree in computer science, or a related field, and at least two years of experience in the field of computer science, focusing on data privacy, computer networking and/or data records management.” Pet., 9 (citing EX1003, ¶22). While I agree that a POSITA would have the education and professional experiences indicated by Petitioner, these experiences alone are insufficient to implement the technology described and claimed in the ’641 Patent. In addition to these experiences, a POSITA would also have familiarity with medical records and databases for storing medical records—particularly in a manner that complies with privacy laws and regulations such as HIPAA. *Id.* The ’641 Patent was not merely solving a computer science problem but was instead addressing such a problem in the context of privacy laws and regulations that would ordinarily prevent entities from analyzing medical data associated with a specific group of individuals. *Id.*

VI. CLAIM CONSTRUCTION

73. Unless otherwise indicated, I have applied the plain and ordinary meaning of the claim terms.

74. Finally, I have reviewed the claim constructions provided in the petition. In my analysis here, I use the same constructions relied on by the Petitioner. These constructions are as follows:

Term	Construction
Token	An identifier associated with an individual that does not reveal the identity of the individual.
Server	A computer, with a processor and memory, on a network that provides information in response to requests from another computer.
Encryption Server	A server that produces tokens in response to a request.
Similarly encrypted	Generated such that tokens generated from corresponding information can be compared to one another to detect a match.
Medical information that characterizes a group	Plain and ordinary meaning that includes information about history of physician visits, medical conditions, procedures performed, prescriptions or disabilities.

VII. THE GROUNDS FOR UNPATENTABILITY

75. The Petition alleges the following grounds for unpatentability:

Ground	Claims	Basis for Alleged Unpatentability
1	1–19	Obvious over U.S. Pat. No. 7,823,207 (“Evenhaim”) (Ex. 1005)
2	1–19	Obvious over Evenhaim in view of U.S. Pat. Appl. Publ. No. US 2007/0294111 (“Settimi”) (Ex. 1006)
3	7–10 and 13	Obvious over U.S. Pat. Appl. Publ. No. US 2002/0111833 (“Dick”) (Ex. 1007) in view of U.S. Pat. No. 7,519,591 (“Landi”) (Ex. 1008)
4	1–6, 11–12, and 14–19	Obvious over Dick in view of Landi and “A Security Architecture for Query Tools used to Access Large Biomedical Databases” by Murphy et al. (“Murphy”) (Ex. 1009)

VIII. THE PRIOR ART

A. Overview of the Evenhaim Reference (EX1005)

76. Evenhaim discloses a system that allows for the searching of PHI at source entities such as pharmacies or healthcare providers. EX1005, 1:14–19, Abstract. Unlike the ’641 Patent, Evenhaim relies on the source entities to search PHI directly and to de-identify patient-level data only after they are searched. EX1005, 6:15–25, 17:43–52.

77. For example, Evenhaim’s system includes an aggregator processor connected to one or more source-entity processors, each source-entity processor corresponding to an organization that maintains PHI for individuals. EX1005,

5:12–28, FIGS. 4, 4A. The aggregator processor receives queries from consumer-entity processors, and from the queries, generates search requests for the source-entity processors. EX1005, 6:56–67, 7:1–27. The source-entity processors search their original micro-level data—including patients’ PHI—to identify records responsive to the search request. EX1005, 6:15–25, 17:43–52. Once patient level data has been identified responsive to the requests, the source-entity processors de-identify those records and return them in “files” to the aggregator processor. EX1005, 7:20–24. The aggregator processor aggregates files received from each of multiple source-entity processors and reports an agglomerated extract of the files to the consumer-entity in response to the query. EX1005, 9:13–27. The aggregator collects and assembles identity protected reports from multiple source entities such that the statistical significance of conclusions are enhanced. *Id.*, 10:7–11.

78. Notably, the search request sent from the aggregator processor to each of the source-entity processors can include a parameter list that carries “privacy sensitive micro-data” such as the names or IDs of individuals (e.g., patients) who are the subject of the request. EX1005, 8:30–48. However, Evenhaim never produces tokens from the patient names in the search request, and Evenhaim’s source-entity processors never match any such tokens to de-identified data records. Evenhaim thus fails to disclose, among other things, an unauthorized party using

an encryption server to query a database for de-identified healthcare information concerning a group of known individuals or a data server producing requested healthcare information that characterizes the group.

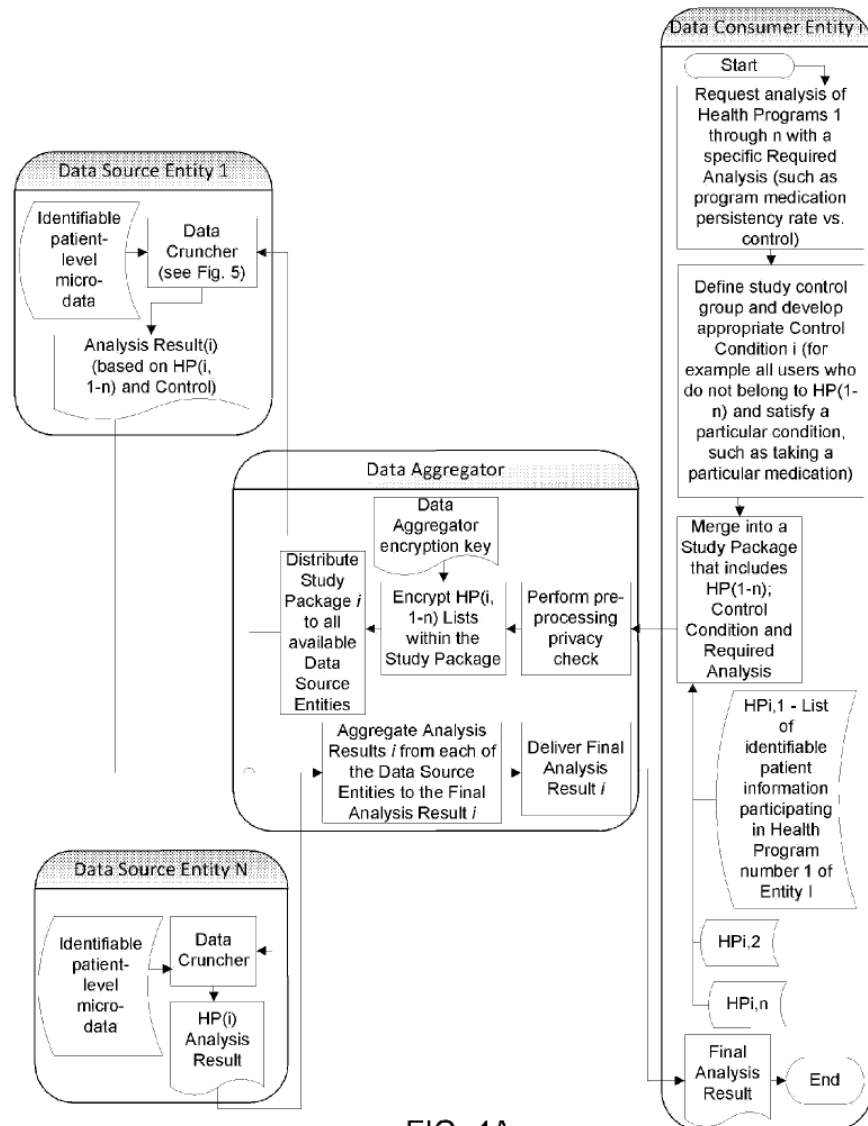


FIG. 4A

Evenhaim, FIG. 4A

79. Evenhaim fails to disclose, among other things, an unauthorized party using an encryption server to query a database for de-identified healthcare

information concerning a group of known individuals or a data server producing requested healthcare information that characterizes the group.

B. Overview of the Settimi Reference (EX1006)

80. Settimi describes systems and methods for searching electronic medical data to identify potential participants for clinical studies. EX1006, Abstract. The method allows for sending de-identified patient information between primary care provider (“PCP”) sites and a data warehouse. EX1006, [0009].

81. Settimi describes a system for generating a cohort report across de-identified patient data stored in a data warehouse. EX1006, [0010] (“In addition, one of the aims of population analysis is to assemble an at-risk cohort population comprised of individuals who may be candidates for clinical intervention.”). In one embodiment, the cohort report can be sent back to a PCP and re-identified at the PCP site. EX1006, [0027]. The de-identification and reidentification process involves encrypting the patient identifier with a unique password *at the PCP site*. EX1006, [0041].

82. Like Evanham, Settimi fails to disclose, among other things, an unauthorized party using an encryption server to query a database for de-identified healthcare information concerning a group of known individuals or a data server producing requested healthcare information that characterizes the group.

C. Overview of the Dick Reference (EX1007)

83. Dick describes computer-based systems and methods for retrieving medical records over a network. EX1007, [0002], [0010], [0021]–[0022]. Dick's topology includes a requesting and viewing client (RVC) 215 connected to a requester's server 230. EX1007, [0020]–[0023], FIG. 3. An example of Dick's topology is shown in FIG. 3, below:

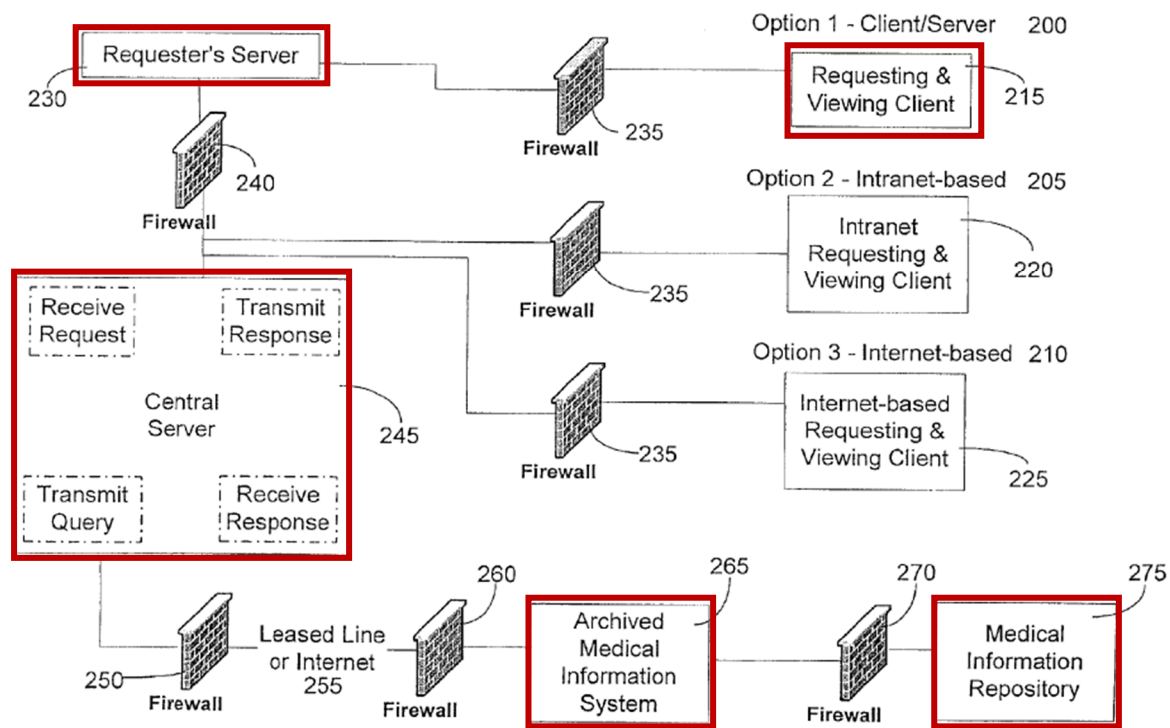


FIG. 3

EX1007, FIG. 3 (annotated)

84. Figure 3 shows three different front-end options. The Petition focuses on Option 1 – Client/Server. Pet. 55. The RVC 215 is “a terminal having at least a video display and keyboard. In general, each RVC is operated by an authorized

user to request and subsequently review retrieved medical information or other search results.” EX1007, [0021]. In Option 1, the RVC 215 “would receive a request from an authorized user responding to prompts from software executing on requester’s server 230.” EX1007, [0022]. Notably, this is the *only* function attributed to the requester’s server 230 in the entirety of Dick’s disclosure.

85. In Dick, “[e]ach request for medical information includes identification of a subject,” where a “subject might consist of a human individual or group of humans.” EX1007, [0024]. Thus, in Dick, the requests do not include tokens or Encrypted IDs, but rather, they include individual identification information or identification information for a group.

86. After the request is received by the requester’s server, the request is sent to the central server 245. EX1007, [0027]. The central server 245 can optionally verify the authenticity of the request. *Id.* Then, the central server 245 sends a query based on the request (the query including the identification of the subject) to a medical information repository (MIR) 275 that stores protected health information for patients.⁴ EX1007, [0028]–[0029]. The MIR 275 locates data

⁴ In other embodiments, the central server 245 sends the query to an archive medical information system (AMIS) server 265 rather than the medical information repository 275 to reduce the computational burden on the medical

records responsive to the query and returns them in a response to the central server 245; the central server then sends the records to the requesting client through the requester's server. EX2002, 75:19–78:19; 93:5–94:7.

87. When the MIR 275 does not have authorization from the subject for the release of their healthcare information, the records are de-identified before release to the central server 245. EX1007, [0045]–[0046], FIG. 2. The central server 245 can optionally apply further processing to the response from the MIR 275 before sending the response to the requester, including “reformatting, searching for and appending names, addresses, phone numbers, fax numbers of physicians or pharmacists referred to in the medical information, and providing interpretive information.” EX1007, [0034]. Dick does not describe tokenization here, nor elsewhere. To the contrary, Dick's searching of medical data records explicitly depends on knowledge of the names or other individual information of any individuals identified in the request. EX1007, [0029] (discussing UMPI and L-MPI).

88. For example, Dick teaches that the central server can even maintain a

information repository 275. EX1007, [0028]. The AMIS server searches using the “identification of an individual for whom a request is being made” and thus the query must include “identification” of the subject. EX1007, [0029].

Universal Master Person Index (UMPI) that includes a set of demographics and other specific information for identifying individuals. EX1007, [0029]. Likewise, the AMIS has a local MPI. *Id.* “The purpose of both instances of the Master Person Index is to enable the identification of an individual for whom a request is being made and to increase the speed and efficiency of retrieval.” *Id.*

89. Dick does discuss de-identification. EX2002, 79:17–81:2. Absent consent for release of medical records, medical records must be de-identified. EX1007, [0045]–[0046]. Dick states that de-identification can occur “at one of any number of points, including being de-identified at the originating source of the information,” *but* “in any case, the information must be de-identified prior to being released or distributed.” EX1007, [0046]. For example, the MIR or the AMIS must de-identify the requested information before returning the information to the central server. *Id.*; EX2002, 77:5–78:19. An important point here is that, in Dick, the searching is performed using names, but the results are de-identified if the query does not also include some indication of patient consent. EX1007, FIGS. 1–2.

D. Overview of the Landi Reference (EX1008)

90. Landi describes “systems and methods that implement secured key encryption for de-identifying patient data to ensure patient privacy, while allowing only the owners of the patient data records and/or other legally empowered entities

to re-identify subject patients of de-identified data records, when needed.”

EX1008, 1:13–22.

91. Landi recognized that by the time of its priority filing in March 2003, approaches to de-identifying information under the HIPAA Privacy Rule were known. Landi perceived a problem with these approaches in that they involved “simply stripping all information from the data records that can be used to determine the identity of the patient, or replacing such patient identifying information with something else” without providing a “mechanism by which patient identification can be recovered, if necessary.” EX1008, 2:19–26. Landi thus proposed techniques for de-identifying PHI that would further allow the PHI to be re-identified by authorized entities as needed. *Id.*, 2:36–40. A core concern of Landi’s was the ability to re-identify patients from de-identified health information, which was purportedly not possible in other de-identification approaches known at the time. EX1008, 2:36–40, 2:49–53, 3:9–13, 3:42–57, 4:28–34, 4:35–48, 4:54–64, 6:56–7:2, 7:30–38, 7:43–48, 8:5–10, 8:16–37, 8:38–55, 9:10–16, 9:36–42, 10:12–14, 10:32–37.

92. Landi’s FIG. 1, reproduced below, illustrates an embodiment of its system:

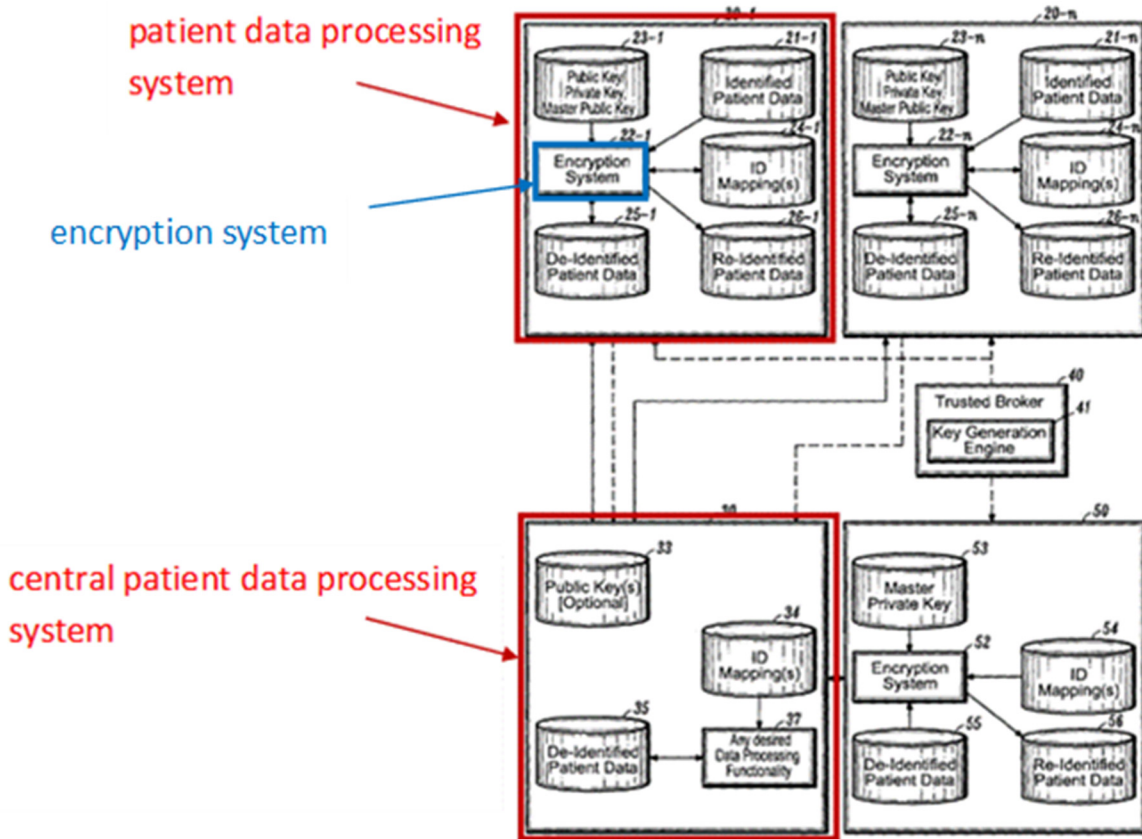


FIG. 1

EX1008, FIG. 1 (annotated)

93. Landi explains that “[t]he patient data processing systems (20-1–20-n) are operated at different clinical sites by different healthcare organizations (including, but not limited to, doctors, healthcare providers, institutions, associations, organizations, hospitals, etc.).” EX1008, 4:19–23. A POSITA would have understood that the patient data processing systems 20-1–20-n correspond to “covered entities” under HIPAA. EX2002, 87:24–88:2. Each patient data processing system (20-1–20-n) includes a respective encryption system (22-1–22-n) that implements a “secure public encryption protocol (e.g., RSA).” EX1008,

4:49–67. The encryption systems (22-1–22-n) “encrypt[] patient identifying information that is stored in (or stored with) the patient data records (21-1-21-n) using respective public keys and/or a master public key (23-1-23-n)” to produce Encrypted IDs. EX1008, 5:3–7; EX2002, 86:25–87:9. Encrypted IDs are stored “with or within a corresponding de-identified [] patient data record (i.e., a patient data records from which patient identifying information has been removed).”

EX1008, 5:32–44. Nowhere does Landi teach or suggest maintaining Encrypted IDs apart from the corresponding de-identified data patient. Nor does Landi ever describe that the Encrypted IDs would be used for “token matching,” despite the Petition’s unsubstantiated assertions to the contrary. *Id.* This is because Landi is not about performing searches or token matching; instead, Landi is simply about de-identifying health records using a technique that facilitates re-identification.

EX1008, 2:36–40, 2:49–53, 3:9–13, 3:42–57, 4:28–34, 4:35–48, 4:54–64, 6:56–7:2, 7:30–38, 7:43–48, 8:5–10, 8:16–37, 8:38–55, 9:10–16, 9:36–42, 10:12–14, 10:32–37. It is a stretch to go from simply storing information in a database to teaching token matching.

94. The encryption system (22-1–22-n) further includes capabilities to “re-identify[] subject patients by using [an] appropriate private key to decrypt de-identified patient data that is contained in de-identified patient data records (25-1–25-n).” EX1008, 6:56–7:2. Landi describes that “holders of valid private keys

(e.g., owners of the patient data, or legally empowered entities) [can] decode the de-identified patient data and re-identify patients.” EX1008, 8:44–46.

95. Landi also provides a central patient data processing system 30 that stores de-identified patient data released from the patient data processing systems (20-1-20-n), “wherein the collected de-identified data records can be processed for purposes of e.g., research, health care monitoring, etc.” EX1008, 4:26–28. Landi emphasizes that “the entity (or entities) that operate the central patient data processing system (30) *does not have the authority to re-identify subject patients* that are associated with the de-identified patient data records (35)” and accordingly, “the central patient data processing system (30) does not include an encryption system that is capable of decrypting Encrypted IDs that are stored in or with the de-identified patient data records (35).” EX1008, 7:22–38.

E. Overview of the Murphy Reference (EX1009)

96. The Murphy references describes “a model for obfuscation of data when served to a client application,” that purportedly “make[s] it extremely unlikely that an individual will be identified.” EX1009, 552. According to Murphy, the model for obfuscation can be applied in a query tool that queries “a clinical data warehouse named the Research Patient Data Registry (RPDR).” EX1009, 552.

97. To “prevent[] the identification of individuals in the database,”

Murphy considered the option of “de-identify[ing] patients in the data base with a system that complies with HIPAA’s 18 points for data de-identification,” but Murphy actually finds this approach problematic. EX1009, 553. Rather than pursue de-identification, Murphy’s query tool only “returns the **number** of distinct patients” identified in the database as matching criteria in the query. *Id.*

Moreover, to prevent users from being able to use the query tool to identify individuals, Murphy proposed an obfuscation method that works by “having the server **not pass true numbers of patients to the query tool**, but rather numbers that would be ... distributed around the true number of patients [if the same query were performed repeatedly].” EX1009, 553–54. Murphy describes using an obfuscation function to “create small values that will be added or subtracted from the true number of patients to prevent patient identification.” EX1009, FIG. 2. “In order to find the true number, one would need to run the same query repeatedly.” EX1009, 554. Murphy’s algorithm would recognize a query run repeatedly as an attack. *Id.* Put simply, Murphy does not return patient records; instead, Murphy returns an obfuscated **number** of patients that would satisfy the query.

98. The Petition cites a scenario in Murphy where the results of a query are close to zero. Pet., 68–69. In that case, Murphy teaches modifying the “range algorithm to have a wider obfuscation at values close to zero, and [indicating] the greater range by returning ‘<3’ when the obfuscated number is less [than] 3.”

EX1009, 555. Note that nowhere in Murphy does it prevent a query based on a number of patients in the query. To the contrary, even if the results to the query are a small (close to zero) number of patients, the Murphy obfuscation algorithm still returns a response. EX1009, 555.

IX. THE CHALLENGED CLAIMS ARE NOT UNPATENTABLE

99. Each ground of invalidity identified above in Section III is incorrect because the prior art in each ground does not disclose at least one limitation of the challenged claims. Additionally, a POSITA would not have been motivated to make any of the proposed combinations with a reasonable expectation of success.

A. Analysis of Ground 1: the Evenhaim Reference Fails to Render Claims 1–19 Obvious

100. The Petition relies on a distorted, hindsight-driven application of Evenhaim that mischaracterizes the reference's express teachings, and indeed, fundamentally alters the system Evenhaim truly describes. Whether borne of a failure to properly understand Evenhaim's disclosure or a flawed attempt to stretch its disclosure onto the challenged claims, the Petition's use of Evenhaim is improper and should be rejected.

101. The overarching distortion presented in the Petition is that Evenhaim somehow discloses an embodiment where the data source entities search de-identified patient records by matching tokens received from the data aggregator with corresponding tokens in a database of de-identified medical records. EX1003,

¶39. But Evenhaim never discloses nor suggests such an embodiment. This embodiment is instead invented entirely by Petitioner and its witness, Dr. Clark, with the '641 claims themselves being the only apparent basis from which this embodiment was injected in Evenhaim.

102. Petitioner's mischaracterization of Evenhaim involves at least three flawed premises: (i) that the data aggregator generates a token for each individual patient in a patient list, (ii) that the generated tokens are distributed in queries from the data aggregator to the data sources entities, and (iii) that the data source entities would match tokens from a query to corresponding tokens in a set of de-identified patient data records. None of these premises are true or supported by Evenhaim, however. They instead derive solely from Dr. Clark's unsubstantiated declaration testimony, which often directly contradict Evenhaim's express disclosures and which, if implemented, would risk HIPAA violations of the type Evenhaim specifically sought to avoid. *See* EX1005, 14:60–63.

1. Evenhaim's data aggregator does not produce a token for each individual included in a group composed of multiple individuals identified in a request

103. The Petition's assertions that Evenhaim's data aggregator produces tokens for individual patients is false. Petitioner and Dr. Clark cite and conflate two distinct contexts in which Evenhaim's data aggregator performs encryption—namely, (1) encryption for data transmission security and (2) encryption for data

mergers—but neither involves creating tokens for individual patients as alleged.

Id.

104. First, consider Evenhaim’s goal of providing data transmission security for communications between the data aggregator and other entities. Evenhaim explains that “it is generally preferable to include some degree of ***data transmission security***” by performing “encryption and decryption” for “every step requiring a ***transmitting*** of data (or of at least one file) and every respective associated step requiring ***receiving*** of that data (or of that at least one file).” EX1005, 13:33-41.

105. Evenhaim’s data transmission security scheme involves encrypting the “patient list and query” that the data aggregator transmits to the data source entities. This is illustrated in FIG. 4, for example, which shows a single “data aggregator encryption key” being applied to encrypt the patient list and query, thereby ensuring that the contents of the patient list and query will not be revealed to unauthorized actors during transmission or revealed until the intended data source entity performs an authorized decryption. But Evenhaim’s data transmission encryption does not involve token production for requested individuals as claimed. Indeed, during his deposition, Dr. Clark himself agreed that Evenhaim supports the interpretation that the patient lists are encrypted to provide data transmission security (EX2002, 43:2-10):

2 Q. Is it possible that the patient list is
3 encrypted to provide data transmission security in
4 Evenhaim?
5 A. Anything is possible. I mean, that's why
6 Evenhaim has so much disclosure.
7 Q. There is nothing that contradicts that
8 understanding in Evenhaim?
9 A. There's -- no, there's certainly -- at least
10 one of the embodiments would function that way.

106. Encrypting entire patient lists (and query), as disclosed in Evenhaim, is far different from producing a token for each patient named in the list, which would be inefficient and unnecessary for data transmission security in any event. Evenhaim is clear that only the patient lists, and not identifiers for each individual in the list, are encrypted at the data aggregator, thus permitting the data source entities to decrypt the lists with an appropriate decryption key. *See, e.g.,* EX1005, 14:3–7 (“*Returning to the abovementioned aspects of preferable encryption*, it is certainly strongly advised that regardless of the general level of encryption elected, *a parameter list including ‘individuals’* should carry a stronger level of *encryption.*”), 15:61–65 (“*Encrypting the lists* using any industry grade encryption method; and Delivering the lists of participants together to a query engine with a capability to *decrypt the lists* at the time of processing ...”), FIG. 5 (showing decryption of each “patient identifier *list*”).

107. Notwithstanding Evenhaim’s seemingly clear disclosure, Petitioner argues that the data aggregator “encrypts the names, which a POSA would understand involves *creating an encrypted token for each individual.*” Pet., 13. The only evidence cited in support of this assertion is the uncorroborated and conclusory declaration testimony of Dr. Clark—which never once acknowledges Evenhaim’s concern with data transmission security or explains how encrypting patient *lists* would include producing tokens for *individual* patients (it does not). *Id.* (citing EX1003, ¶¶41, 44-45). Although Dr. Clark admits during deposition that the encryption of the patient list could be merely for the purpose of providing data transmission security, neither his declaration nor the Petition makes any attempt to explain why a POSA would abandon such a common-sense read of Evenhaim—which would be supported by the intrinsic disclosure of the reference—to adopt the convoluted token production and matching theory that finds no support within the four corners of the reference.

108. Neither Petitioner nor Dr. Clark can square their assertion with the words of the reference itself, which describes encrypting the patient *list* and query, rather than producing tokens for individual patients. Nor can the Petition or Dr. Clark support their contention that any alleged tokens resulting from encryption of the patient list would be compared to corresponding tokens for de-identified patient data at the source entities. *Id.* This theory assumes that alleged tokens from the

patient list would not be decrypted by the data source entities since those tokens would be compared to corresponding tokens, but Evenhaim explicitly teaches the contrary: “every step requiring a transmitting of data ... and every respective associated step requiring receiving of that data ... may preferably include respective encryption *and decryption*.” EX1005, 13:33–36, FIG. 5.

109. The Petition’s and Dr. Clark’s additional citations to Evenhaim’s “interim data merger enabled embodiments” are similarly unavailing and fail to show that the data aggregator ever generates encrypted tokens for individuals identified in a request that would be sent in a query to any data source entity. EX1003, ¶39; EX1005, 12:4–13:20. As an initial matter, Evenhaim’s “interim data merger enabled embodiments” involve encryption in an entirely different context from encrypting the patient list and query for data transmission security, as described elsewhere in Evenhaim. Indeed, as noted above, the patient lists encrypted at the data aggregator for data transmission security are *decrypted* by the data source entities, while the data merger enabled embodiments discussed in col. 12 of Evenhaim specifically cautions that the party receiving the encrypted data should *not* be capable of decrypting that data. *Compare* EX1005, 13:33–35 (“every step requiring a transmitting of data ... preferably include[s] respective encryption *and decryption*”) and 15:63 (“decrypt the *lists*”) with 12:16–20 (“special care must be taken that the entity performing the linkage is *not capable*

of knowing the key and decryption function; because knowing these facets would enable a breach of the individual’s privacy”). It would be non-sensical for the data source not to decrypt a patient list and query that the aggregator has encrypted for data transmission security. The notion that decrypting patient lists at the source entity would implicate a breach of privacy of the type described at col. 12:16–20 is similarly non-sensical, especially as the patient list contains no PHI and Evenhaim expressly discloses embodiments where such decryption is performed without breaching patient privacy. *See, e.g.,* EX1005, FIG. 5 (“Decrypt patient identifier list”). Petitioner’s and Dr. Clark’s arguments ignore these facts and repeatedly conflate encryption for data transmission security with the encryption described at column 12 of Evenhaim.

110. To be clear, Evenhaim never once discloses or suggests that its “interim data merger embodiments” would involve the data aggregator producing tokens for individual patients that would be shared with the data source entities as alleged. Dr. Clark repeatedly cites Evenhaim’s statement that “the encryption of individual identification and/or merger of data for individuals could be facilitated ... on the ‘aggregator’ processor side” (*see* EX1005, 12:24–29), but this one line is far too vague to support anything like the detailed scheme that Petitioner and Dr. Clark attempt to inject into Evenhaim as part of their mapping to the ’641 claims. Evenhaim instead discloses that “encryption and/or merger” on the data aggregator

can occur during the steps of “receiving a respective file, or aggregating the plurality of files,” while conspicuously omitting any mention of the aggregator encrypting the identities of each patient in the patient list itself. EX1005, 12:30–32. The steps of “receiving a respective file, or aggregating the plurality of files” notably occur upon the aggregator’s receipt of *response(s)* to the queries and are not at all related to encrypting the query itself. *See id.*, 7:3–6, FIG. 3. It would make no sense for the data aggregator to produce a token for each patient in the patient list that it sends with the query to the data source entities, especially since the patient list and query themselves contain no PHI that would require de-identification under HIPAA. The data source entities also already know the patients’ identities and maintain their PHI, and there is simply no reason that the data aggregator would need to disguise the identities of the patients in a request that contains no PHI from data source entities that already maintain PHI for the patients.

111. Dr. Clark also appears in one instance to recognize that the above-quoted portion of Evenhaim refers to a linking process at the data aggregator, not token matching at the data source. In an apparent effort to reconcile this with the erroneous “token matching” interpretation, Dr. Clark refers to an alleged “*additional* level of security” that could be “added to the token matching system” to provide “a second level of protection.” EX1003, ¶42. Specifically, Dr. Clark

states: “the tokens in the patient records could be further de-identified with a second encryption key that is only available to the data source. This allows for records belonging to the same patient to be matched for further analysis on the encryption server, but still prevents any reverse engineering of the identity back to the tokens.” EX1003, ¶42. I disagree. The second level of protection that Dr. Clark refers to here is not described in Evenhaim and only highlights that additional “fixes” would be required if token matching were to be performed at the data source entities. The fact that these “fixes” are never addressed in Evenhaim itself provides further evidence that Evenhaim never contemplated having the data source entities search on de-identified data records using token matching.

112. I also disagree with Dr. Clark’s assertion that “a POSA would understand matching tokens is preferable to matching re-identified PII because when using the tokens the information would not need to be de-identified for the request, re-identified for the matching, and de-identified again for the response, and therefore using tokens is more efficient and further ensures compliance with HIPAA.” EX1003, ¶[0040]. The problem that Dr. Clark alludes to here does not exist because Evenhaim does not send individual tokens from the aggregator to the data source entities in the first place. This problem again only arises if one accepts the false premise that Evenhaim would send such tokens to the data source entities in a query. Evenhaim does not do so, and the lack of any acknowledgement or

proposed solution to this problem in Evenhaim further confirms that Evenhaim does not operate as alleged in the Petition.

113. Producing tokens for individual patients at the data aggregator to query the data source entities is also non-sensical because it would require the data source entities to take inefficient steps of either (i) decrypting the tokens before searching for the appropriate patients' data records or (ii) pre-generating corresponding tokens for patient data records that could be compared against the tokens received from the data aggregator. Considering the significance of these steps, one would reasonably expect Evenhaim to describe them, or even mention them at all, if the interim-data merger enabled embodiments were intended to cover Petitioner's interpretation. But Evenhaim is entirely silent in this regard. Worse, the embodiment invented in the Petition would itself risk a HIPAA violation if the data source entities released de-identified patient data to the data aggregator that included the patient's token, as would occur to permit linking of data records at the aggregator. EX1005, 12:53–13:20. In this case, the data aggregator would be capable of comparing the token it received from the source entity to the token it earlier sent in the queries, thereby permitting the aggregator to correlate the patient's name or other identifier from the patient list to de-identified patient level data released from the source entities in violation of the patient's privacy and regulations such as the HIPAA Privacy Rule. *Id.*

2. Evenhaim’s data aggregator does not convey request tokens for individual patients to data source entities

114. Even if Petitioner’s assertion that Evenhaim generates individualized tokens for each patient in the patient list were taken at face value (which it does not), Evenhaim does not disclose, and it still would not have been obvious, to query the data source entities with those tokens in Evenhaim’s system.

115. For context, Petitioner’s witness, Dr. Clark, contends that Evenhaim “produce[s] encrypted tokens *that are distributed as a query to the data sources.*” EX1003, ¶40. Dr. Clark appears to infer this position solely from Evenhaim’s disclosure that “[t]here are numerous locations where an encryption of individual identification ... could be facilitated,” including on the ‘aggregator’ processor side.” EX1005, 12:24-34. But this terse disclosure does not support Dr. Clark’s position. Nowhere does Evenhaim imply that the output of such encryption is either (i) distributed to the data sources or (ii) used in token matching at the data sources. Indeed, such distribution of individually encrypted tokens from the aggregator to the data sources would be absurd in the context of Evenhaim’s system for multiple reasons. *Id.*

116. First, no need exists for the data aggregator to provide the data sources with tokens produced by individually encrypting the patient names or IDs rather than simply providing the patient names or IDs themselves. The patient list and query do not include protected health information (PHI) that would ordinarily

dictate a need for de-identification under applicable privacy laws such as HIPAA at least because the names do not originate with a covered entity and they are not obtained from patients' private medical information. *Id.* They are simply names or IDs of individuals whose de-identified medical data is requested. EX1005, 7:8:4–5 (“Intrinsically, in the context of the instant invention, the parameters of the list may include identity disclosing specifics”), 8:10-48. By contrast, the data source entities are the entities that originate and maintain PHI in Evenhaim. EX1005, 5:12–28. Data source entities are “organizations that generate, capture, or store (for example, in the health care industry) medical and claims data that includes identifiable personal health information.” *Id.* Data source entities include physician offices, hospitals, labs, pharmacies, and other “Covered Entities” as defined under HIPAA. *Id.*, 5:15–19. As the originators and maintainers of PHI, these entities already know the patients' names and PHI. Requiring the data aggregator to replace patient names with tokens in the request would be nonsensical. Indeed, any attempts to conceal the patient names from the data source entities would be futile, as the data sources already possess this information. *Id.*

117. To this point, Dr. Clark's statements that “the query sent from the aggregator to the data sources should not include personally identifying information” and “transmitting personally identifying information to the data

source as part of the query could itself be a potential HIPAA violation” is patently false. EX1003, ¶40. As noted above, the data source entities themselves are “covered entities” under HIPAA (EX1005, 5:12–19), and there can be no HIPAA violation in transmitting a query that contains no PHI to the data sources.

118. More, and ironically, it is Petitioner’s invented embodiment that is nowhere disclosed in Evenhaim that actually raises the specter of a HIPAA violation. Under Petitioner’s theory, the data aggregator would both (i) produce tokens from a patient list and (ii) receive matched tokens from the data source entities, thereby rendering the data aggregator capable of recovering patient identities by correlating patient names with returned records from the data source entities without authorization. Yet Evenhaim itself warns that the data aggregator or Crossix protocol operator should not be provided medical data from which the identities of individuals could be reasonably derived: “[w]hen releasing data from the data source to the data aggregator, ***the personal IDs will be encrypted—but using the same key*** in all data sources—***a key that will preferably not be known to the Crossix protocol operator... .***” EX1005, 12:61–66; *see also, id.*, 12:16–20 (“special care must be taken that the entity performing the linkage is not capable of knowing the key and decryption function; because knowing these facets would enable a breach of the individual’s privacy”). HIPAA’s de-identification standard specifically states that de-identification must be accomplished such that there “is

no reasonable basis to believe that the information can be used to identify an individual.” EX1005, 2:10–12; 45 C.F.R. §164.514(a). But Petitioner’s and Dr. Clark’s proposal to return matched tokens with de-identified health data to the same entity—i.e., the data aggregator—that creates the request tokens in the first place makes it almost certain that the data aggregator could identify individuals and their corresponding healthcare data. Pet. 21, 24; EX1003, 40. This example also highlights the unreliability of Dr. Clark’s opinions that are underpinned by significant misunderstandings of HIPAA and privacy concerns in general. In this context, and further considering his lack of citations to third-party corroborating evidence or other authority, Dr. Clark’s opinions are entitled to little or no weight. Fed. R. Evid. 702(b); 37 C.F.R. §42.65(a).

119. Evenhaim’s data aggregator also would not convey request tokens to the data source entities because the data source entities are configured to search original micro-level patient data from which patient names or IDs in the request can be matched against patient names or IDs in the data source entities’ original data records. EX1005, 6:15–34, 9:47–51, 17:41–52. There is no token matching at the data source entities in Evenhaim not only because it is unnecessary, but also because it would be contrary to Evenhaim’s specific goal of searching original micro-level patient data *before it is de-identified or aggregated*. *Id.*; see also EX1005, 17:47–48 (“This analysis is performed on the original, most complete

data set”). In fact, any encryption of individually identifying information to produce tokens is only performed by the data sources *after the relevant data records have already been identified* for release to the data aggregator and not for the purpose of matching to identify patient data records as alleged: “[A]t substantially each data source there is preformed [sic] *a name matching to identify all of the records* for a certain identity (e.g. for Jane Doe). ... *When releasing data from the data source to the data aggregator, the personal IDs will be encrypted-* but using the same key in all data sources—a key that will preferably not be known to the Crossix protocol operator, but only a trusted third party such as an escrow agent.” EX1005, 12:53–66. Evenhaim thus teaches away from the exact approach that Petitioner and Dr. Clark improperly seek to inject in Evenhaim’s system to force a read on the challenged claims of the ’641 Patent.

120. Evenhaim also specifically illustrates in FIG. 5 a data cruncher module of a data source entity that decrypts a patient identifier list for the very purpose of allowing names from the lists to be matched against names in the original data records. EX1005, Fig. 5. In fact, name matching or matching based on similar individually identifying information is the only approach described in Evenhaim for processing the queries received at the data source entities. See EX1005, 9:47–51 (“If the parameter list included specific individuals by name or ID or the likes, “Crunching together” may involve *name matching through “fuzzy*

logic” and other name matching algorithms of the population defined by the parameter list with the source-entity database names, in addition to the other steps defined above.”). By contrast, Evenhaim describes no embodiment where Petitioner’s proposed “token matching” occurs at the data source entities. This again is not surprising, as Evenhaim specifically sought to have the data source entities respond to queries based on analysis of *raw data* in its original, most detailed form. EX1005, 6:16–17 (“the instant invention allow[s] analysis of ‘source-entity’ raw data at is original, most detailed form (high resolution data) including full access to all of the privacy sensitive data currently at its disposal . . .”). Evenhaim distinguishes its proposed invention from prior approaches by specifically calling for de-identification to occur *after name-matching and analysis have been completed on the raw data*:

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, 17:42-52.

121. For at least these reasons, Evanhaim fails to even suggest, let alone describe that any tokens produced by the aggregator are distributed as a query to the data sources.

3. Evenhaim’s data source entities do not perform the alleged “token matching” to search de-identified healthcare data

122. The Petition cites Dr. Clark’s declaration testimony that “[t]here is an embodiment [in Evenhaim] that does not require tokens, but Evenhaim also describes using a token matching system to allow for querying de-identified patient records.” EX1003, ¶19. But this is wrong; the latter embodiment simply does not exist.

123. The portion of Evenhaim (12:36–42) that Dr. Clark refers to for this assertion does disclose two embodiments, but not as Dr. Clark characterized them. Evenhaim in fact discloses “two different situations where data *from the data source* is returned already aggregated, after analysis as well as a second option where data is released at the micro-level (each person’s data), but the person identity information, for the matched population, is replaced with a unique encryption key, such as a hash or Advanced Encryption Standard (AES) or the likes [sic].” EX1005, 12:35–42.

124. Thus, the first embodiment involves data being aggregated at the data source before it is returned to the data aggregator, and the second situation involves de-identifying individual patient level data that can be returned to the data

aggregator and later merged or linked by the aggregator itself. Notably, neither situation involves the data source entities performing token matching on de-identified patient data as alleged. Dr. Clark’s characterization of these embodiments is completely at odds with Evenhaim’s actual disclosure. EX1003, ¶40.

125. The portion of Evenhaim that Dr. Clark cites states that “the person identity information ... is replaced with a unique encryption key,” but nothing in Evenhaim discloses or suggests that such replacement is to allow the unique encryption key (i.e., the alleged token) to be matched to another token in a query received from the aggregator. Even the sentence that Dr. Clark quotes in support of his position—“the person identify information, *for the matched population*, is replaced with a unique encryption key,” (EX1003, ¶40, citing EX1005, 12:39–41)—indicates that the individuals *are first matched* to determine the matched population before the person identity information, for the matched population, is replaced with a unique encryption key. As such, because the “token” is not even produced at the data source until after a matching population is already identified, the portions relied on by Petitioner’s witness cannot logically describe any token matching as alleged.

126. Dr. Clark also distorts Evenhaim’s descriptions of data linking *at the aggregator* to wrongly contend that the data source entities would create tokens

associated with patient healthcare data for a matching process. *See* EX1003, ¶40

(“this token matching system ‘preserves the ability to known [sic] that two records belong to the same identity, but preserves the privacy of the identity of that person.”). *Id.*, 12:42–45. But Dr. Clark fails to acknowledge that Evenhaim is instead referring to the ***aggregator’s*** (not the data sources’) ability to link de-identified patient records belonging to the same patient:

If the data sources are careful to encrypt the identifying portions of each record using a common encryption “key”, then further down the data processing circuit it will be possible to link records related to a common individual without compromising the identity of that individual. Of course, special care must be taken that the entity performing the linkage is not capable of knowing the key and decryption function;

EX1005, 12:12–18.

127. Evenhaim’s separate references to the “data sources” and the entity that is “further down the data processing circuit,” make clear that the latter entity is different from the data sources. And because Evenhaim seeks to prevent the compromise of individual identities at the entity “further down the processing circuit,” the phrase cannot encompass the data sources, which themselves are covered entities under HIPAA that are already aware of such identities and already maintain PHI. EX1005, 5:12–28. As such, Dr. Clark’s statement that a “POSA would understand that ‘further down the data processing circuit’ describes the subsequent use of the de-identified records for querying,” is simply incorrect. At

the very least, the cited portions of Evenhaim do not show that any token matching would take place at the data sources.

128. Indeed, when asked during his deposition, the only portion of Evenhaim that Dr. Clark was able to identify as purportedly describing token matching (“Column 7, starting at about 39”) pertained to systems that were prior art to Evenhaim - not the data source which he otherwise proclaims as performing token matching (EX2002, 55:3–16, 56:6–13):

3		That there is express disclosure of the case	
4		where the tokens could be on the source entity side, in	
5		which case that matching the query of that data would	
6		have to occur there. Then that's an express disclosure.	
7		Q. And can you point me to that express	
8		disclosure?	
9		A. I've already done so.	
10		Do you want me to search again?	
11		Q. Yes, please.	
12		A. So Column 7, starting at about 39, it	
13		describes how the source entities could protect the	
14		privacy of the PII fields, which they would do by	
15		creating a token.	
16		So there's your explicit disclosure.	

...

6	Q. Were there any other portions of Evenhaim that
7	disclosed matching at the source entities?
8	A. There may be. That's the one I found. I'm
9	not really inclined to search the whole reference.
10	Q. Are you aware of any other citations in your
11	declaration to portions of Evenhaim disclosing matching
12	of the source entities?
13	A. Not from memory, no.

129. Dr. Clark’s attempt to repurpose a discussion of prior art systems as somehow also describing the invention in Evenhaim, and his inability to point to a single other portion of Evenhaim that discloses token-matching at a source entity is telling. It is, however, not surprising because Evenhaim fails to disclose or render obvious multiple limitations of independent claims 1, 7 and 14

130. For each of the reasons described above (*supra*, §IX.A.1–2), Evenhaim fails to disclose or render obvious multiple limitations of independent claims 1 and 7. For example, Petitioner equates the data aggregator of Evenhaim to “an encryption server.” Pet., 13. However, because Evenhaim does not describe that the data aggregator produces individual tokens either from the patient list and query or as part of the data-merger embodiments, Petitioner has not, and cannot, show that Evenhaim provides “an encryption server... for producing a token for each individual included in a group composed of multiple individuals,” as recited in elements [7.a]–[7.b] (and similarly in [1.b]–[1.c] and [14.c]–[14.d]).

Pet., 17–18, 30.

131. Further, Petitioner equates Evenhaim’s data source entities to the “data server.” Pet., 19. However, because Evenhaim fails to describe any matching of request tokens from the data aggregator to tokens for de-identified healthcare data at the data source entities, Petitioner has not, and cannot, show that Evenhaim provides “a data server for producing the requested healthcare information... by identifying the tokens in the set of de-identified healthcare data ... that correspond to the produced tokens,” as recited in elements [7.e]–[7.g] (and similarly in [1.f]–[1.g] and [14.f]–[14.g]). Pet., 19–20, 30.

132. Neither would the foregoing features be obvious over Evenhaim. To the extent Petitioner argues that it would have been obvious to modify Evenhaim to have the data source entities search de-identified healthcare information based on matching tokens associated with the de-identified healthcare information to request tokens from the data aggregator, the contention is unsubstantiated and improper. As described above, Evenhaim explicitly teaches against such an approach that would require the data sources to search on anything but the original micro-level patient data. *Supra*, §IX.A.1–2. Moreover, common knowledge of a POSITA may only be used to supply a missing claim limitation when that limitation is “unusually simple and the technology particularly straightforward.” The Petition both fails to present any evidence that the above-noted limitations that are missing

from Evenhaim were commonly known in the art and fails to show that these limitations are directed to unusually simple features. They are not. Evenhaim's system would require a substantial re-design to implement the embodiments that Petitioner and Dr. Clark attempt to import in the reference, which would require sophistication and complexity to achieve a technical design that both achieved Evenhaim's specific goals and complied with applicable privacy laws and regulations. This is anything but simple. *Id.*

133. For each of these reasons, Petitioner has failed to establish that independent claims 1 and 7 are obvious over Evenhaim. Each of the dependent claims inherit the novelty and non-obviousness of the corresponding independent claim, and thus have not been shown to be obvious either. Ground 1 of Petitioner's challenge should therefore be dismissed.

4. Evenhaim fails to disclose or render obvious multiple limitations of independent claims 1, 7 and 14

134. For each of the reasons described above (*supra*, §IX.A.1–3), Evenhaim fails to disclose or render obvious multiple limitations of independent claims 1 and 7. For example, Petitioner equates the data aggregator of Evenhaim to “an encryption server.” Pet., 13. However, because Evenhaim does not describe that the data aggregator produces individual tokens either from the patient list and query or as part of the data-merger embodiments, Petitioner has not, and cannot, show that Evenhaim provides “an encryption server... for producing a

token for each individual included in a group composed of multiple individuals,” as recited in elements [7.a]–[7.b] (and similarly in [1.b]–[1.c] and [14.c]–[14.d]). Pet., 17–18, 30.

135. Further, Petitioner equates Evenhaim’s data source entities to the “data server.” Pet., 19. However, because Evenhaim fails to describe any matching of request tokens from the data aggregator to tokens for de-identified healthcare data at the data source entities, Petitioner has not, and cannot, show that Evenhaim provides “a data server for producing the requested healthcare information... by identifying the tokens in the set of de-identified healthcare data ... that correspond to the produced tokens,” as recited in elements [7.e]–[7.g] (and similarly in [1.f]–[1.g] and [14.f]–[14.g]). Pet., 19–20, 30.

136. Neither would the foregoing features be obvious over Evenhaim. To the extent Petitioner argues that it would have been obvious to modify Evenhaim to have the data source entities search de-identified healthcare information based on matching tokens associated with the de-identified healthcare information to request tokens from the data aggregator, the contention is unsubstantiated and improper. As described above, Evenhaim explicitly teaches against such an approach that would require the data sources to search on anything but the original micro-level patient data. *Supra*, §IX.A.1–3. Moreover, common knowledge of a POSITA may only be used to supply a missing claim limitation when that limitation is

“unusually simple and the technology particularly straightforward.” The Petition both fails to present any evidence that the above-noted limitations that are missing from Evenhaim were commonly known in the art and fails to show that these limitations are directed to unusually simple features. They are not. Evenhaim’s system would require a substantial re-design to implement the embodiments that Petitioner and Dr. Clark attempt to import in the reference, which would require sophistication and complexity to achieve a technical design that both achieved Evenhaim’s specific goals and complied with applicable privacy laws and regulations. This is anything but simple. *Id.*

137. For each of these reasons, Petitioner has failed to establish that independent claims 1 and 7 are obvious over Evenhaim. Each of the dependent claims inherit the novelty and non-obviousness of the corresponding independent claim, and thus have not been shown to be obvious either. Ground 1 of Petitioner’s challenge should therefore be dismissed.

B. Analysis of Ground 2: the Evenhaim-Settimi Combination Fails to Render Claims 1–19 Obvious

138. In Ground 2, the Petitions contends that the teachings of Evenhaim in view of Settimi would have rendered the claims of the ’641 Patent obvious. Pet., 34–51. In the proposed Evenhaim-Settimi combination, the Petition explains that Settimi’s central patient data warehouse would replace the individual data source entities in Evenhaim and the central patient data warehouse would search de-

identified patient records by matching tokens representative of patients whose data was requested to stored tokens associated with the patients' de-identified records: "Once de-identified and stored in the central repository, the healthcare records *can be queried using a token matching scheme.*" Pet., 35; EX1003, ¶52. According to the Petition, "Settimi describes *querying* the de-identified patient records *by using the token (EPID)* to find the associated records for a specific patient without revealing the patient's identity." *Id.* The premise that Settimi describes token matching at the central warehouse is wrong, however, and is based on further mischaracterizations of the prior art.

139. Settimi is in fact directed to systems and methods for identifying patient candidates for clinical studies. EX1006, Abstract. Electronic medical data is stored in a central data warehouse—but because it is obtained from patient care providers (PCPs) who are subject to patient privacy laws such as HIPAA, the PCPs deidentify patient records data before the data is exported to the central data warehouse for storage. *Id.*, [0009]. De-identification is accomplished by removing identifying information from the medical records and generating an encoded patient ID for each record, referred to as an EPID. *Id.*, [0038]. The Petition equates Settimi's EPID to the claimed "token." Pet., 35. However, a proper understanding of the query process in Settimi, which is not addressed in the Petition, makes clear that not only does Settimi fail to describe matching EPIDs to

retrieve data records, but the use of EPIDs for querying would be purely non-sensical in Settimi’s system, let alone in the Evenhaim-Settimi combination.

1. The Evenhaim-Settimi combination fails to disclose or render obvious multiple limitations of independent claims 1, 7 and 14

140. In more detail, Settimi describes techniques for querying de-identified medical data stored in the central warehouse to surface patients who fit the clinical trial criteria specified in the request. For example, to identify candidate patients for a clinical trial, a user can query for “patients with a particular disease that were treated with a particular medication,” “patients of a particular age and sex who have particular test results,” or “all women with heart disease who are taking a hormone replacement therapy drug.” EX1006, [0036]. A cohort of patients who meet the conditions specified in the request are identified from de-identified medical records stored in the central warehouse, and an indication of the cohort is returned to the requester or the primary care provider (PCP)—although only the PCP has the ability to re-identify patients by decrypting the EPIDs. *Id.*, [0037].

141. Importantly, Settimi’s queries necessarily include and rely on patient characteristics to identify the cohort because Settimi attempts to eliminate the traditional “use of mass media to broadcast a need *for patients who fit a list of clinical conditions.*” EX1006, [0011]. Querying the database of Settimi using EPIDs—as Petitioner contends—would be non-sensical at least because EPIDs do

not represent patient characteristics or clinical conditions that would allow for identification of a cohort for clinical trials or other research as intended. EX1006, [0038]. Rather, as Petitioner and Dr. Clark admit, the database in Settimi is searched using a “common vocabulary” that normalizes terminology in the data from multiple sources. Pet., 36; EX1003, ¶137. Petitioner does not contend (and it would be meaningless to do so) that this common vocabulary includes EPIDs. It does not. Indeed, if particular EPIDs that fit the clinical study requirements were known to the entity generating the query, there would be no reason for the query in the first place. Accordingly, much like Evenhaim, Settimi never discloses querying a database for de-identified healthcare data using tokens or performing so-called “token matching” at a de-identified data server, and Petitioner’s premise for combining the two references— namely, that “a POSA would readily understand that the search would involve matching the tokens sent in the query to the tokens already in the relevant healthcare record” is not correct. Pet., 41; Ex. 1003, ¶153.

142. For at least these reasons, Settimi cannot cure the deficiencies of Evenhaim, and the Evenhaim-Settimi combination fails to render obvious at least “a data server for producing the requested healthcare information... by identifying the tokens ... and ... de-identified healthcare data that correspond to the produced tokens,” as recited in elements [7.e]–[7.g] (and similarly in [1.f]–[1.g] and [14.f]–

[14.g]). Pet., 40–41, 46. Settimi likewise does not disclose “an encryption server[] ... for producing a token for each individual included in a group,” as recited in elements [7.a]–[7.b] (and similarly in [1.b]–[1.c] and [14.c]–[14.d]), and neither the Petition nor Dr. Clark rely on Settimi for the encryption server features that are already lacking from Evenhaim. Pet., 37–39; EX1003, 139–144; EX2002, 97:1–8.

2. The Evenhaim-Settimi combination would not have been obvious because integration of Settimi’s teachings would have violated Evenhaim’s express preference for searching original, micro-level patient data

143. The Petition’s proposed combination of Evenhaim and Settimi would not have been obvious to a POSITA for the additional reason that it would have violated Evenhaim’s express preference and principle of operation for searching on original, micro-level data before de-identification and aggregation. EX1005, 6:15–34 (“instant invention allow[s] analysis of ‘source-entity’ raw data at its original, most detailed form (high resolution data) including full access to all of the privacy sensitive data currently at its disposal”), 17:42–52 (“analysis is performed on the original, most complete data set”), 17:28–41 (contrasting Evenhaim’s purported invention with “classic” approaches that called for “aggregation of de-identified patient” before searching).

144. For example, regarding the combination, the Petition contends that “[o]nce de-identified and stored in the central repository, the healthcare records can be queried using a token matching scheme ... using the token (EPID) to find

the associated records for a specific patient without revealing the patient's identity." Pet., 35. As described in the preceding section, Settimi never actually discloses searching the data warehouse using the token (EPID). But even if Settimi did disclose these features, the combination still would have required a non-obvious modification to Evenhaim's system in light of Evenhaim's desire to search "raw data at its original, most detailed form." The data records stored in Settimi's central warehouse are not maintained in their original, most detailed form and do not include PHI. Not only is the data de-identified, thereby leaving the data records without useful information that Evenhaim sought to make available for search, but Settimi confirms that the data imported to the data warehouse before a search would be performed is aggregated, cleansed, and normalized—all contrary to Evenhaim's express teachings. EX1006, [0035] ("The data import function 206 *aggregates* and *cleanses* de-identified patient data from multiple sites and then stores the data into a staging area 208. Data received from multiple PCP systems 108 is *normalized*" and "*combined together* into a relational database"). Ground 2 thus fails for this additional reason.

C. Analysis of Ground 3: the Dick-Landi Combination Fails to Render the Challenged Claims Obvious

145. The Petition fails to show that the challenged claims are unpatentable over the Dick-Landi combination for multiple reasons, as described below.⁵

1. The Petition fails to show that a POSITA would have combined Dick and Landi in a manner that would lead to the claimed invention

146. The Petition fails to establish that a POSITA would have combined Dick and Landi to arrive at the claims of the '641 Patent. First, the Petition erroneously asserts that “Dick does not describe any specific de-identification methods” and that a POSITA would need to look beyond Dick’s disclosure to understand how de-identification could be performed Pet.52; EX1003, ¶¶201–203; EX2002, 79:17–81:2. To the contrary, Dick provides extensive description for how to de-identify health information. The Petition’s entire basis for turning to Landi to augment Dick’s disclosure thus rests on a false premise that would not have been obvious to a POSITA.

147. For example, Dick teaches that de-identification can involve only removing names or addresses of patients, but also removing “all ‘Identifying’

⁵ The deficiencies described in this section are similarly applicable to the claims challenged in Ground 4 based on the Dick-Landi-Murphy combination.

information” such as:

identifiers of the individual or of relatives, employers, or household of members of the individual associated with the record, which identifiers include names, geographic subdivisions, elements of dates related to any individual, telephone numbers, fax numbers, e-mail addresses, Social Security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate license numbers, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, photographic images, any other unique identifying number, characteristic or code.

148. EX1007, [0045]. Even Landi recognizes that “[c]onventional methods for de-identifying patient data include *simply stripping all information* from the patient data records that can be used to determine the identity of a patient,” like in Dick. EX1008, 2:19–26. In this way, Dick teaches de-identification techniques sufficient for a POSITA to perform de-identification on health information. EX1007, [0045]; EX1008, 2:19–26; EX2002, 79:17–81:2:

11 Q. Would a person of skill know how to implement
12 the de-identifying methodologies?
13 A. Should.

21 Q. Would a person of skill see a need to look
22 beyond the Dick reference itself to implement
23 de-identifying methodologies?
24 A. No. I think a person of skill would have
25 knowledge of HIPAA and the need to de-identify data.

EX2002, 80:11–25.

149. Further, Dick goes beyond “simply stripping” identification information, as Landi puts it. Dick teaches a mechanism for de-identification technique for situations when removing information “is not practical or renders the data useless.” EX1007, [0045]. Therefore, a POSITA would have found the de-identification methodology taught by Dick sufficient, and would not have needed to look elsewhere. EX2002, 79:17–81:2.

150. As can be seen, Dick *does* describe de-identification methods. *See*, EX1007, [0045]–[0047]. Thus, contrary to the Petition’s proposition, a POSITA reading Dick would have no reason to look elsewhere for de-identification methodology. EX1003, 201; EX2002, 79:17–81:2.

151. Second, the Petition’s proposal to integrate Landi’s encryption system in Dick’s requester’s server over a concern that sending PII in a query “would potentially” violate HIPAA is unfounded. Pet. 57. It is not a HIPAA violation to

send PII in a query that lacks PHI. EX2002, 57:16–25; EX2006, §164.514(d).

152. Third, adding Landi’s de-identification methods to Dick’s system as proposed in the Petition and Dr. Clark’s declaration would itself implicate HIPAA violations that a POSITA would have sought to avoid. Fourth, neither the Petition nor Dr. Clark explain why a POSITA would have been motivated to turn to Landi, specifically, or how the Landi reference improves upon what is already disclosed in Dick. For these reasons, and those described in further detail elsewhere, a POSITA would have lacked the motivation to combine Dick and Landi in the manner proposed in the Petition. *Id.*

2. The Dick-Landi combination does not disclose or render obvious elements [1.b]–[1.c], [7.a]–[7.b], or [14.c]–[14.d]: an encryption server for producing a token for each individual included in a group identified in a request for healthcare information

153. The Petition fails to establish that the Dick-Landi combination discloses or renders obvious “an encryption server, having a processor and a memory, for producing a token for each individual included in a group composed of multiple individuals identified in a request for healthcare information that characterizes the group,” as recited in elements [7.a]–[7.b], or similarly recited in [1.b]–[1.c] and [14.c]–[14.d]. To reach these claim elements, the Petition argues that it would have been obvious to implement an encryption server akin to Landi’s encryption system 22 in Dick’s requester’s server 230. Pet., 55–57. But this

assertion is misplaced for multiple reasons described in detail below.

154. At the outset, neither Dick nor Landi individually describes an encryption server that produces a token for each individual included in a group identified in a request for healthcare information, as claimed. At best, Landi describes an encryption *system* located only within a patient data processing system 20-n—a covered entity under HIPAA—and nowhere else. EX1008, 4:49–54, 5:7–13 (describing that the “healthcare entity” can use its own public key to generate an Encrypted ID), 5:32–41 (describing the data processing system generating Encryption IDs and storing them in a repository), 6:56–7:2 (describing that each healthcare entity that releases de-identified patient data records can securely store a respective private key for purposes of re-identifying patient data); FIG. 1; EX2002, 86:25–87:7 (describing encryption occurring at the patient data processing systems in Landi).

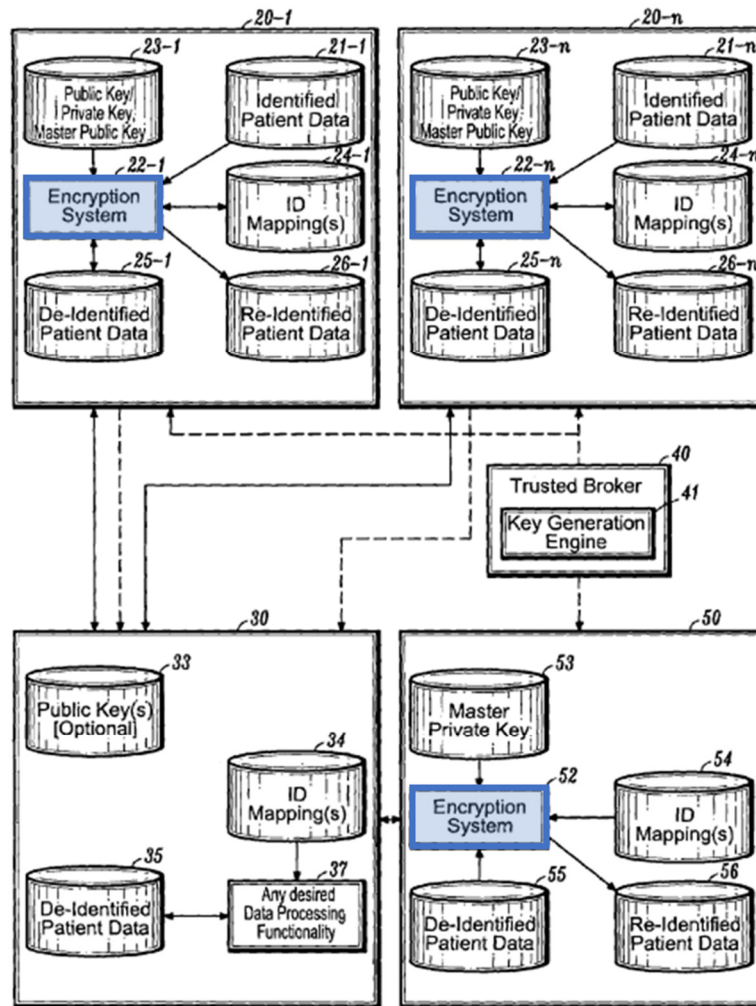


FIG. 1

EX-1008, FIG. 1 (annotated).

155. First, the Petition's proposal to place the encryption system of Landi at the requester's server of Dick is predicated *entirely* on an assumed need for the requester's server to provide tokens rather than patient names to the next server in the network (e.g., Dick's central server 245 or Landi's central system 30). Pet., 57–58 (“it would potentially violate HIPAA to just send PII to be used for such a

query directly to the centralized data server”). But that need is entirely illusory, conspicuously devoid of evidentiary support. To the contrary, as verified by Dr. Clark, there is no HIPAA violation in sending only PII in a query to the requester’s server:

16	Q. Sure. So I'll rephrase my question.
17	Are you -- are you aware of any provisions of
18	HIPAA that would be violated by a noncovered entity
19	transmitting patient names to covered entities?
20	A. I mean, I'd have to look at the specific
21	example. But if you just sent the name and didn't have
22	the healthcare data with it in any way, then it wouldn't
23	violate. But if you link that with any medical
24	procedure or any healthcare information, then you would
25	have a HIPAA violation.

EX2002, 57:16–25

156. There is NO rule in HIPAA that prevents the transmission of PII in a query when the query includes no PHI. EX2006, 164.514(d). This so-called “potential” HIPAA violation simply does not exist as a problem in the prior art. Without this stated problem, the Petition cannot support the claim that a POSITA “would have been motivated to use Landi’s encryption server to produce tokens to query against a de-identified patient database requester.” Pet. 53 (citing EX1003, ¶203).

157. Dr. Clark confirmed that the encryption system of Landi could have been placed at the central server of Dick, and the system would still be HIPAA compliant.

3 Q. But as described at paragraph 214, you've
4 proposed to place Landi's encryption system in Dick's
5 requester's server; is that correct?
6 A. That's one way to do it. As I'm looking at it
7 now, it's probably -- be even easier to just plug it at
8 the Central Server. But either way would work.
9 Q. You did not describe the option of modifying
10 the Central Server to include encryption server in your
11 declaration?
12 A. Either one works. As we discussed, the
13 requester's server is just routing the request. So you
14 could -- you could plug in the system of Landi at either
15 place, and it would function the same.
16 Q. And the system would still be HIPAA compliant
17 even if encryption were performed at the Central Server
18 rather than the requester's server?
19 A. As long as there -- the PII was protected and
20 it was designed to only return de-identified
21 information, yes, it would be compliant.

EX2002, 92:3–21.

158. Thus, even Petitioner's expert agrees that the absence of an encryption system at the requester's server would not be problematic for HIPAA compliance.

159. In addition, the Petition suggests potential HIPAA violations by sending PII to the centralized server but does not recognize or discuss whether

sending PII to the requester's server would likewise violate HIPAA. Pet. 57. This glaring inconsistency is easily explained by the Petition's hindsight reasoning to shoehorn Landi's encryption system into Dick's requester's server for the sole purpose of reading the combination onto the claims. As is discussed later, placement of Landi's encryption system into Dick's requester's server would create a HIPAA privacy problem, and therefore, a POSITA would not have done so.

160. Second, the Petition's placement of the encryption system at the requester's server relies on impermissible hindsight to map the prior art onto the claims. Landi describes the encryption system 22-1–22-n as being for de-identifying (and re-identifying) patient records at the patient data processing systems 20-1–20-n, and stores the Encrypted IDs with or in patent data records. EX1008, 5:3–7, 5:32–47, 6:56–65, 7:26–30, 8:38–55, 13:4–12; EX2002, 86:9–87:9. The patient data processing systems 20-1–20-n are covered entities under HIPAA, per Dr. Clark. EX2002, 87:24–88:2. Landi's makes it clear that the encryption system performs de-identification at a covered entity that also stores PHI. Nowhere in Landi does it describe the encryption systems as being configured to generate tokens from a received query and to send the query onwards. Nor does it describe placing the encryption system anywhere else besides a covered entity for the purposes of de-identifying patient data. The

Petition's departure from the teachings of Landi to place the encryption system at the requester's server relies entirely on impermissible hindsight reasoning in an attempt to map the prior art to the claims.

161. Third, the proposed combination would also result in a violation of patients' privacy rights under HIPAA or other applicable regulations due to the fact that the requester's server would hold all three pieces of information at the same time: the names of the patients received from the request, the corresponding encrypted IDs, and the patients' de-identified healthcare information received in the response. EX2002, 76:6–78:19. The MIR/AMIS being covered entities would not be permitted to send de-identified medical information to the requester's server because the requester's server is not authorized to have such information. EX2002, 74:9–17. Dick never proposed that the requester's server would maintain patients' PHI, and the Petition has certainly not established that the requester's server would be authorized to do so. EX2002, 71:20–72:6. Accordingly, it would be impermissible for the MIR/AMIS to release all of this information to the requester's server that could be used to link patient names with their corresponding healthcare records. This clear privacy and HIPAA violation means that a POSITA would not consider this option at all.

162. The Petition avers that, to avoid HIPAA violation, it was “common practice to use a public encryption key to create tokens on a requesting server

when sending a query,” without any evidentiary support. Pet. 57–58 (citing to EX1003, ¶214, which does not mention anything about the practice of creating tokens). At best, the Petition cites to a paper from 1988 (before HIPAA existed) and to another paper from 2008 that deals with credit card security, neither of which have been authenticated. EX1011–EX1013. Regardless, the Petition relies on the combination of Dick and Landi, neither of which teach this feature. The Petition then resorts to specious conclusions drawn from blatant mischaracterizations of both the prior art and the HIPAA privacy rules.

3. The Dick-Landi combination does not disclose or render obvious elements [1.f], [7.e]–[7.f], [14.f]: identifying tokens in a set of de-identified healthcare data that correspond to request tokens for individuals in a group

163. The Dick-Landi combination does not disclose or render obvious “producing the requested healthcare information that characterizes the group by identifying the tokens in the set of de-identified healthcare data and the associated de-identified healthcare data that correspond to the produced tokens” (elements [1.f], [14.f]) or “a data server for producing the requested healthcare information that characterizes the group by identifying the tokens in the set of de-identified healthcare data and the associated de-identified healthcare data that correspond to the produced tokens” (element [7.f]). Despite assertions to the contrary, neither Dick nor Landi disclose these features.

164. As an initial matter, the claims are not directed to mere “token

matching” or de-identification techniques as alleged in the Petition. *See* Pet., 6, 52, 59, 63. The claims instead apply these techniques in a novel combination and context in which, among other things, requested healthcare information is produced by identifying the tokens in a set of de-identified healthcare data that correspond to tokens produced for individuals identified in a request for healthcare information that characterizes a group. The Petition has not demonstrated that Landi teaches or suggests these claim features.

165. For example, the Petition cites to Landi, 8:23–55 and 11:23–29 for these features. Pet., 62–63. But these portions of Landi do not involve matching tokens in the manner claimed, or even matching Encrypted IDs. This portion of Landi instead describes how the use of the same encryption algorithm and public key to encrypt the same PII from two or more data records belonging to the same patient will produce the same Encrypted ID, thereby ensuring consistency *in the assignment* of Encrypted IDs to the same patients’ records from different providers or at different times. EX1008, 8:23–55 (Since the encryption is reproducible, the same patient can be recognized at different times (i.e., *consistent de-identification can be achieved* over episodic collection events) even though the identity of the person remains unknown.”), 11:3–29 (describing step 53 where Encrypted IDs are generated by the encryption system at the patient data processing system, and clarifying that the “process ensures that if data is collected more than once *from a*

particular patient, the patient will be mapped to the same Encrypted ID”). This mapping and generation of Encrypted IDs, and collection of patent records, notably occurs at the patient data processing system 20-1–20-n, and not at the central patient data processing system 30. *Id.*, 8:23–55, 11:3–29, cls.1,3,12,15.

166. The Petition’s additional citation to Landi’s Claim 15 is deficient for similar reasons. Pet., 58–60. The operations described in claim 15 would be performed at the patient data processing systems 20-1–20-n where de-identification and re-identification occur, and do not involve matching encrypted IDs in a query to encrypted IDs associated with de-identified health care data stored in the central patient data processing system 30. *See*, EX1008, 8:49–55, cl. 1,3,12,15.

167. In addition, Landi does not teach querying the central system 30. At best, Landi teaches that “structured” patient data records can be “readily searched” for the purposes of de-identification at the patent data processing system 20-1–20-n. EX1008, 11:52–63. Likewise, unstructured patient data records can be searched for the same purpose. EX1008, 13:13–40. But Landi does not suggest querying the central patient data processing system 30, and it is wrong to assume that Landi teaches token matching when it doesn’t even teach querying based on the Encrypted IDs.

168. In short, the Petition has not shown that the Dick-Landi combination discloses or renders obvious the claimed operations for identifying tokens in a set

of de-identified healthcare data that correspond to the produced tokens according to the features recited in elements [1.f], [7.e]-[7.f], and [14.f].

4. The Dick-Landi combination does not disclose or render obvious elements [1.h], [7.h], [14.h]: the produced healthcare information is absent personally identifiable information

169. During his deposition, Dr. Clark clarified that in Landi, as applied to the combination, personally identifiable information (PII) is not “absent” from the produced healthcare information. Instead, the PII remains in the produced healthcare information as encrypted information (e.g., an encrypted ID). EX2002, 86:9–24. Additionally, as mentioned before, Landi’s encryption methodology is designed to permit de-identification of PII. *See, supra* §VIII.D. Thus, consistent with Dr. Clark’s explanation, PII would be available in the produced healthcare information and could be read simply by applying the decryption algorithm and re-identification techniques expressly described in Landi. EX1008, 2:36–40, 2:49–53, 3:9–13, 3:42–57, 4:28–34, 4:35–48, 4:54–64, 6:56–7:2, 7:30–38, 7:43–48, 8:5–10, 8:16–37, 8:38–55, 9:10–16, 9:36–42, 10:12–14, 10:32–37. The Dick-Landi combination therefore does not teach that the PII is absent from the produced healthcare information as claimed in elements [1.h], [7.h], or [14.h].

5. Landi’s method of de-identification does not satisfy HIPAA requirements

170. The Petition contends that “Landi describes a token matching system

used to de-identify medical records, such as the records referred to in Dick. Ex.

1003, ¶¶58, 202.” Pet., 52. “Landi describes how different healthcare organizations de-identify their records by creating an encrypted token (an encrypted form of the PII such as a name or SSN).” Pet., 52. The Petition proposes that a POSITA reading Dick would turn to Landi for implementing de-identification. Pet., 52.

171. It may be true that “different healthcare organizations de-identify their records by creating an encrypted token,” but this proposed method of de-identification is not compliant with HIPAA. Pet., 52; §164.514 (b). Specifically, encryption of “patient identifying information” i) does not meet the de-identification standards of §164.514(b) (stating the two HIPAA approved methods of de-identification), ii) does not meet the re-identification requirements of §164.514(c)(1) (stating “[t]he code or other means of record identification is not derived from or related to information about the individual”), iii) does not meet the requirements of §164.514(a) establishing the standard for de-identified data (“Standard: De-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.”).

172. A POSITA would have understood Landi’s description of “de-identifying (encrypting)” as just that: encrypting. Because a POSITA would have

recognized that Landi’s de-identification techniques were not HIPAA compliant, a POSITA would not have elected to use them in combination with another reference, like Dick.

173. Dr. Clark refers to Landi, 4:40–46 and 11:23–29, which state that “public keys ... are used for *de-identifying (encrypting)* one or more items of patient identifying information (i.e., information that could be used for identifying the patient) to generate an encrypted version of the patient identifying information (referred to herein as “Encrypted IDs)” Landi, 4:35–48. Thus the Petition and Dr. Clark have not addressed why Dick would teach a technique for de-identification and then turn to Landi that de-identifies i) by a different method and ii) in a method not compatible with HIPAA.

6. The Dick-Landi combination results from impermissible hindsight.

174. I have been informed that impermissible hindsight exists in an obviousness analysis when the Petition or expert provides no basis for their modifications or combination other than what the subject patent describe. Here, the proposed Dick-Landi combinations are replete with impermissible hindsight. To understand the hindsight reasoning, we consider the implications of combining Landi with Dick in each of several possible implementations of the Dick-Landi

combination.⁶ *Id.*

a. No encryption server would have been necessary in the Dick-Landi combination

175. Neither Dick nor Landi expressly teaches an encryption server that produces a token for each individual included in a group identified in a request for healthcare information, as claimed. At best, Landi describes an encryption *system* residing within a patient data processing system 20-n, which would be a covered entity under HIPAA, and nowhere else. EX1008, 4:49–54, 5:7–13 (describing that the “healthcare entity” can use its own public key to generate an Encrypted ID), 5:32–41 (describing the data processing system generating Encryption IDs and storing them in a repository), 6:56–7:2 (describing that each healthcare entity that releases de-identified patient data records can securely store a respective private

⁶ The Petition is unclear as to how the combination is actually implemented. For example, the Petition vaguely contends that a “POSA would have readily understood that Landi’s manner of storing de-identification data could be used ***with or in place of Dick’s repository.***” Pet., 61 (citing EX1003, ¶221); EX2002, 91:13–94:7. Elsewhere, Dr. Clark argues that “a POSA would [understand] that Landi’s central database/system, 30 could ***replace Dick’s central server 245.***” EX1003, ¶213.

key for purposes of re-identifying patient data), 8:47–55 (describing that the public keys are used to de-identify patient data), FIG. 1; EX2002, 86:5–87:7 (describing encryption occurring at the patient data processing systems in Landi).

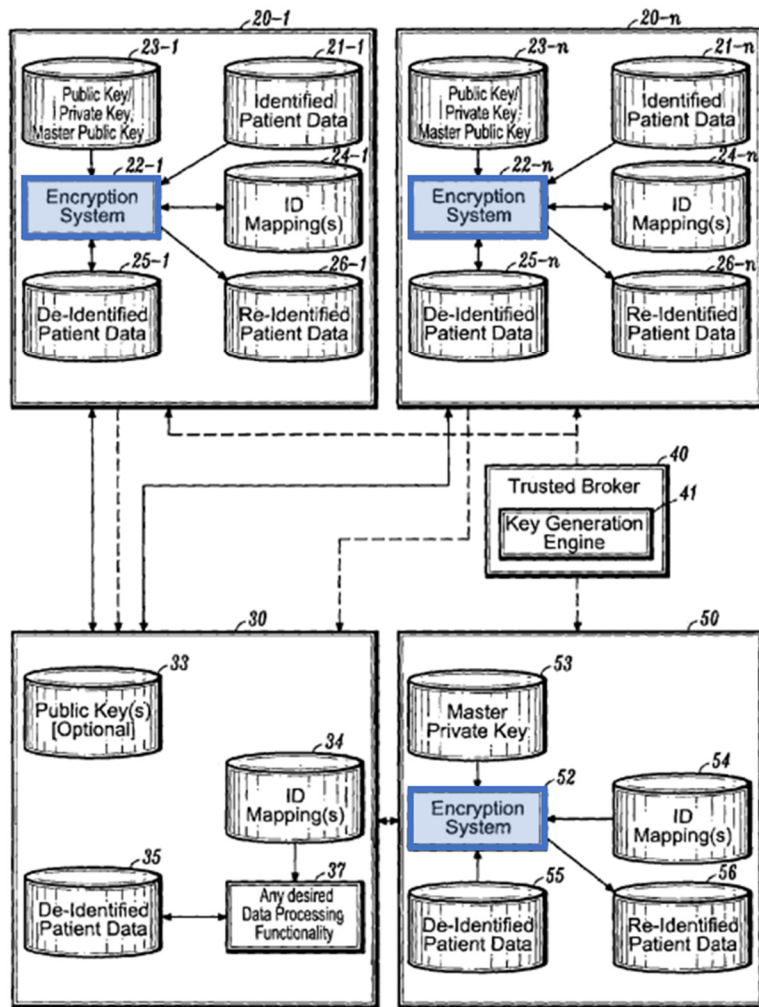


FIG. 1

EX-1008, FIG. 1 (annotated).

176. Petitioner’s proposal to place the encryption system of Landi at the requester’s server of Dick is predicated on an alleged need for the requester’s

server to provide tokens rather than patient names to the next server in the processing network (e.g., Dick’s central server 245 or a patient data repository). But that need does not exist and producing tokens from the requester’s server would serve no purpose at all. To understand why, we consider the implications of placing an encryption system for producing tokens at Dick’s requester’s server in each of several possible implementations of the Dick-Landi combination. Because the Petition does not make it clear how the combination is actually implemented, various possibilities that I could best glean from the record are addressed here.⁷ *Id.*

(1) Non-obvious Under Combination Possibility 1: Dick’s MIR or AMIS Includes Landi’s Manner of Storing De-identification Data

177. In the first possible implementation of the combination, Landi’s manner of storing de-identification data is used *with* Dick’s repository. Pet., 61. As best we understand, this implementation would involve using Landi’s database

⁷ For example, the Petition vaguely contends that a “POSA would have readily understood that Landi’s manner of storing de-identification data could be used *with or in place of Dick’s repository*.” Pet., 61 (citing EX1003, ¶221); EX2002, 91:13–94:7. Elsewhere, Dr. Clark argues that “a POSA would [understand] that Landi’s central database/system, 30 could *replace Dick’s central server 245*.” EX1003, ¶213.

35 for storing de-identified patient data in Dick’s MIR (element 275 in FIG. 3) or AMIS (element 265 in FIG. 3).

178. First, Dick already teaches de-identifying information in the MIR or AMIS prior to distributing medical information. EX1007, [0046] (describing that “the information *must be* de-identified prior to being released or distributed”).

Thus, a POSITA would have understood that Dick already teaches some form of electronic medium in Dick’s MIR or AMIS for storing de-identified information, like a database. Therefore, a POSITA reading Dick would have recognized that there was no need to add *another* database (like Landi’s de-identified patient data 35) to Dick’s system for storing de-identified information—such a medium already exists in Dick.

179. Second, Dick already teaches the following:

- 1) The requests made to the MIR or AMIS use identifiable patient information (EX1007, [0024]);
- 2) The MIR or AMIS stores medical information, which are accessed by the central server 245 (EX1007, [0027]–[0028]);
- 3) Searching is done at the AMIS or MIR using identifiable patient

information (via a master person index (MPI)⁸) (EX1007, [0028]–[0031]);

4) The MIR or AMIS performs de-identification prior to distributing data (EX1007, [0046]); and

5) The MIR or AMIS returns de-identified patent information to the requester’s server, through the central server, in response to the search. (EX1007, [0046]; EX2002, 75:19–78:19; 93:5–94:7).

180. Considering these teachings from Dick, a POSITA would have recognized that in Dick, *no encryption server would have been needed* to create tokens for performing searches at the MIR or AMIS. This is because the MIR and AMIS are already capable of 1) receiving PII in a request; 2) searching using PII (e.g., using the MPI); 3) performing de-identification (with or without Landi); and 4) returning the requested de-identified health information. Adding an encryption server at the requester’s server would have added complexity and cost to a system that was designed to work without it; thus, a POSITA would not have done so.

181. The Petition’s proposed addition of the encryption server to the

⁸ The purpose in both instances of the Master Person Index (MPI) is to enable the identification of an individual for whom a request is being made and to increase the Speed and efficiency of retrieval.” EX1007, [0029].

requester's server, therefore, amounts to impermissible hindsight with the only apparent purpose of facilitating Petitioner's attempt to map disconnected elements of Dick and Landi onto the claims. As mentioned before, neither Dick nor Landi teaches the claimed encryption server, which generates tokens after receiving a request. To arrive at the claimed encryption server, the Petition makes an inferential leap that is unsupported by the actual teachings of Dick and Landi. *Id.*

(2) Non-obvious Under Combination Possibility 2: Replace Dick's MIR or AMIS with Landi's Manner of Storing De-identification Data

182. In the second possible implementation of the combination, Landi's manner of storing de-identification data is used *in place of* Dick's repository. Pet., 61; EX2002, 92:22–93:22. As best we understand, this implementation would involve replacing Dick's MIR or AMIS with Landi's central patient data processing system 30, which includes the database of de-identified data 35. But the proposal to provide Landi's encryption system at Dick's requester's server in this context is a non-starter.

183. For example, viewed through the lens of HIPAA, Dick's MIR and AMIS are both covered entities because they store protected health information (PHI) (medical information that can be identified to a person). EX2006, §164.514(d) (describing the requirements for protecting PHI). Specifically, Dick's MIR and AMIS store identifiable patient data that can be de-identified for release

to third parties. EX1007, [0028]–[0031]. In this respect, the MIR/AMIS are analogous to Landi’s patent data processing system 20-n, which also maintain PHI. EX2002, 85:15–86:8.

184. By contrast, Landi’s central patient data processing system 30 never has access to PHI, and all PHI must be removed before being sent to the central patient data processing system 30. EX1008, 7:3–38. Indeed, according to Landi, central patient data processing system 30 “does not have the authority to re-identify subject patients that are associated with the de-identified patient data records (35) containing de-identified (encrypted) patient identifying information.” EX1008, 7:22–38. The Petition fails to explain why a POSITA would have sought to fundamentally alter the character of Dick’s system by searching Landi’s central patient data processing system 30 rather than the AMIS or MIR (covered entities) that were already capable of storing PHI and de-identifying PHI when responding to queries. *Id.*

185. In one possible implementation of the combination, Landi’s central server 30 replaces Dick’s AMIS. In this context, Dick’s MIR also would have had to be altered to include the encryption system 22-1–22-n to create the de-identified health information. EX1008, 4:65–7:2. But the Petition has not established that a POSITA would have added the encryption system 22-1–22-n of Landi to Dick’s MIR. A POSITA reading Landi would have understood Landi’s manner of storing

de-identification data to involve 1) creating de-identified information using an encryption system 22-n at a patient data processing system 20-n, 2) storing the de-identified data records 25-n, and 3) transmitting the de-identified data records to the central server 30 for storage in a database 35. EX1008, 4:49–64, 14:26–33.

This would require adding the encryption system 22-1–22-n and other components of Landi’s patient data processing system 22-1–20-n to Dick’s MIR, which is something the Petition has not established. Accordingly, the Petition has not established that a POSITA could not have reasonably substituted the Dick’s AMIS with Landi’s central patient data processing system 30; to the contrary, the Petition itself states that the reason Landi would have been needed was because Dick did not teach methods of de-identification. The Petition’s failure to include the encryption server 22-1–22-n into Dick’s MIR illustrate the lack of reasoning and support behind their specious combinations.

186. If only the databases of Landi were included in the combination, no mechanism would exist to produce the de-identified patient data with the Encrypted IDs, according to the Petition. At best, the Petition makes a blanket statement that “a POSA would have been motivated to use Landi’s de-identification system in which PII is encrypted to form an Encryption ID and the de-identified records are stored in a central database for querying.” Petition, 53 (citing EX1003, ¶203). That statement by itself does not constitute an explanation

of how the MIR would function in the combination. Indeed, this appears to be yet *another* proposal, where the entire de-identification system (the patent data processing system, the central patient data processing system 30, the trusted broker 40, etc.) is incorporated into Dick somehow. Even then, the Petition does not provide any explanation of how that would work, resulting not only in ambiguity, but also insufficient reasoning to explain how and why a POSITA would have made the combination. Last, it has not been established that any searching is performed on Landi's central patient data processing system 30. For example, Appendix B shows the actual text for each citation in the Petition and Declaration pertaining to token matching. Even if a POSITA would have implemented the combination, no encryption server would have been needed: Dick's MIR can run searches without Encrypted IDs, and Landi's central patient data processing system 30 includes public keys, which can generate Encrypted IDs locally prior to performing any searching. EX1007, [0042]; EX1008, 7:30–34.

187. Assuming that the Petition's characterization of the availability of Landi's public keys is correct,⁹ the placement of the public keys in Dick would be arbitrary. And placing them at the requester's server is not the best option—unless you are trying to map the prior art to the claims. For example, Dick contemplates

⁹ I do not concede this point.

each RVC is operated by an authorized user to request and subsequently review retrieved medical information or other search results.” EX1007, [0021]. Thus, the requester is authorized to view medical information and have PII. EX1007, [0021], [0024]. By placing the public keys with the requester, a POSITA would have recognized that the requester could have generated Encrypted IDs before sending the request to the requester’s server—something Dick contemplates the requester legally being able to do. By doing so, the PII in the query never leaves the safety of the requester. Placing the public keys at the requester’s server 230 of Dick, however, would immediately expose the PII to network insecurities.

188. In addition, the Petition suggests potential HIPAA violations by sending PII to the centralized server but does not recognize or discuss whether sending PII to the requester’s server would likewise violate HIPAA. Pet. 57. This glaring inconsistency is easily explained by the Petition’s hindsight reasoning to shoehorn Landi’s encryption system into Dick’s requester’s server for the sole purpose of reading the combination onto the claims. As is discussed later, placement of Landi’s encryption system into Dick’s requester’s server would create a HIPAA privacy problem, and therefore, a POSITA would not have done so.

(3) Non-obvious Under Combination Possibility 3: Landi's Central Database/System 30 Replaces Dick's Central Server 245

189. Dr. Clark (not the Petition) further proposes replacing Dick's central server 245 for Landi's central database system 30. EX1003, ¶213 ("Further, a POSA would find understand that Landi's central database/system, 30 could replace Dick's central server 245."). Because this option was not raised in the Petition, it is waived. Nonetheless, this option would apparently involve bodily incorporation of Landi's central patient data processing system 30 into Dick's environment 200, entirely replacing Dick's central server 245, as shown below:

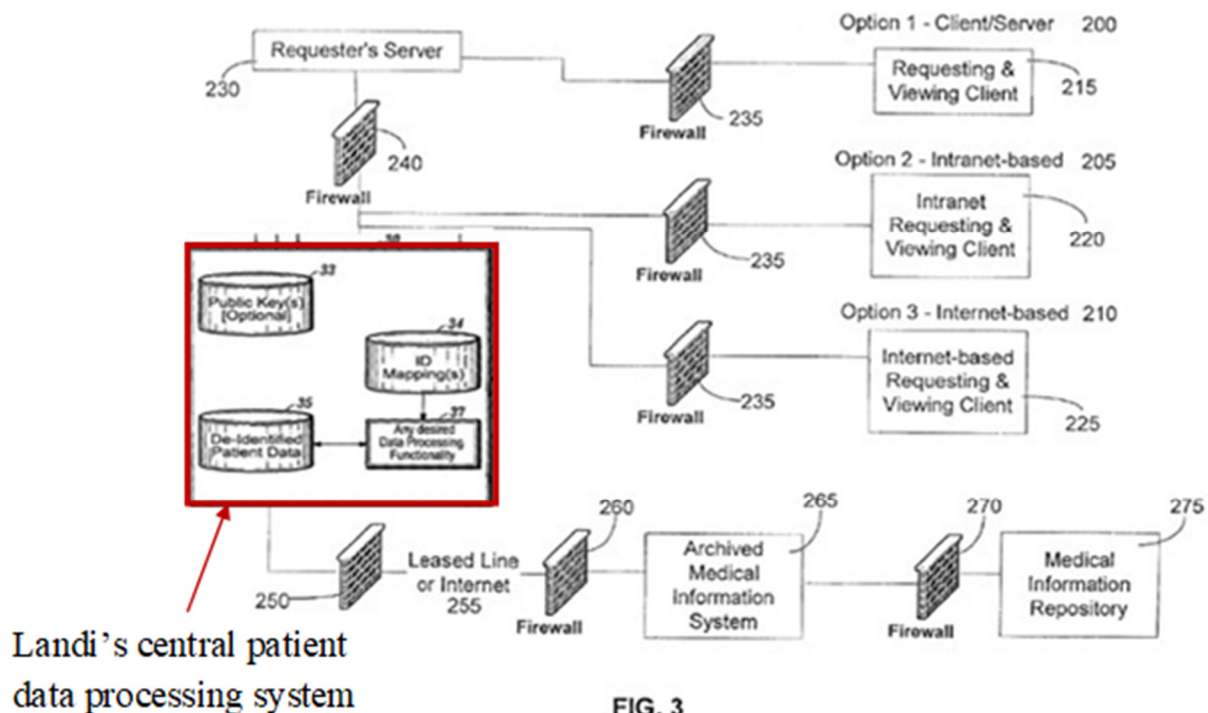


FIG. 3

Dick FIG. 3 with Landi's Central Patient Data Processing System 30

Here, Dr. Clark's wholesale replacement is not workable on its face because Landi does not describe the central patient data processing system 30 as performing any of the functions lost when Dick's central server 245 is replaced.

190. For example, Dick describes the central server 245 as performing request verification, transmitting a query to a medical information repository 275 or AMIS for information pursuant to the request 115, preparing a response to the request received from the RVC, formatting the response, reformatting, searching for and appending names, addresses, phone numbers, fax numbers of physicians or pharmacists referred to in the medical information, and providing interpretive information. EX1007, [0027]–[0028], [0032]–[0034]. At best, Landi describes its central patient data processing system (30) as having “one or more data processing engines (37) that are used for processing the de-identified patient data (35) for one or more given applications.” EX1008, 7:7–10. The Petition and Dr. Clark have not shown that Landi expressly teaches the requisite features of Dick's central server 245; nor have the Petition or Dr. Clark discussed how or why a POSITA would have modified Landi's central patient data processing system to perform the functions of Dick's central server 245.

191. Additionally, in this proposal, Landi's central database 30 is coupled to Dick's requester's server. Neither Landi nor Dick describe the central server as being able to communicate directly with the RVC. Landi does not describe any

external communication pathways into or out of the central patient data processing system 30 (besides the patient data processing system and the central surveillance system). In Dick, the central server 245 communicates with the RVC 215 only through the requester's server 230. EX1007, [0022], [0027], [0032]–[0033].

192. The proposed combination would result in a violation of patients' privacy rights under HIPAA or other applicable regulations due to the fact that the requester's server would hold all three pieces of information at the same time: the names of the patients received from the request, the corresponding encrypted IDs, and the patients' de-identified healthcare information received in the response.

EX2002, 93:5–94:7. The MIR/AMIS being covered entities would not be permitted to send de-identified medical information to the requester's server because the requester's server is not authorized to have such information. Dick never proposed that the requester's server would maintain patients' PHI, and the Petition has certainly not established that the requester's server would be authorized to do so. 2002, 71:20–72:6. Accordingly, it would be impermissible for the MIR/AMIS to release all of this information to the requester's server that could be used to link patient names with their corresponding healthcare records. This clear privacy and HIPAA violation means that a POSITA would not consider this option at all.

b. Placement of the encryption server is arbitrary

193. Assuming that the Petition’s characterization of the placement of Landi’s encryption system is correct,¹⁰ then placement of the encryption server in Dick’s system would be arbitrary. And placing them at the requester’s server is not the best option—unless you are trying to map the prior art to the claims. For example, Dick already contemplates each RVC being operated by a user authorized to request and subsequently review retrieved medical information or other search results. EX1007, [0021]. Thus, the requester is authorized to view medical information and have PII. EX1007, [0021], [0024]. By placing the public keys with the requester, a POSITA would have recognized that the requester could have generated Encrypted IDs before sending the request to the requester’s server—something Dick contemplates the requester legally being able to do. By doing so, the PII in the query never leaves the safety of the requester. Placing the public keys at the requester’s server 230 of Dick, however, would immediately expose the PII to network insecurities.

194. In addition, the Petition suggests potential HIPAA violations by sending PII to the centralized server but does not recognize or discuss whether sending PII to the requester’s server would likewise violate HIPAA. Pet. 57. This

¹⁰ I would not concede this point.

glaring inconsistency is easily explained by the Petition’s hindsight reasoning to shoehorn Landi’s encryption system into Dick’s requester’s server for the sole purpose of reading the combination onto the claims. As is discussed later, placement of Landi’s encryption system into Dick’s requester’s server would create a HIPAA privacy problem, and therefore, a POSITA would not have done so.

c. Landi’s method of de-identification does not satisfy HIPAA requirements

195. The Petition contends that “Landi describes a token matching system used to de-identify medical records, such as the records referred to in Dick. Ex. 1003, ¶¶58, 202.” Pet., 52. “Landi describes how different healthcare organizations de-identify their records by creating an encrypted token (an encrypted form of the PII such as a name or SSN).” Pet., 52. The Petition proposes that a POSITA reading Dick would turn to Landi for implementing de-identification. Pet., 52.

196. It may be true that “different healthcare organizations de-identify their records by creating an encrypted token,” but this proposed method of de-identification is not compliant with HIPAA. Pet., 52; §164.514 (b). Specifically, encryption of “patient identifying information” i) does not meet the de-identification standards of §164.514(b) (stating the two HIPAA approved methods of de-identification), ii) does not meet the re-identification requirements of §164.514(c)(1) (stating “[t]he code or other means of record identification is not

derived from or related to information about the individual”), iii) does not meet the requirements of §164.514(a) establishing the standard for de-identified data (“Standard: De-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.”).

197. A POSITA would have understood Landi’s description of “de-identifying (encrypting)” as just that: encrypting. Because a POSITA would have recognized that Landi’s de-identification techniques were not HIPAA compliant, a POSITA would not have elected to use them in combination with another reference, like Dick.

198. Dr. Clark refers to Landi, 4:40–46 and 11:23–29, which state that “public keys ... are used for *de-identifying (encrypting)* one or more items of patient identifying information (i.e., information that could be used for identifying the patient) to generate an encrypted version of the patient identifying information (referred to herein as “Encrypted IDs)” Landi, 4:35–48. Thus the Petition and Dr. Clark have not addressed why Dick would teach a technique for de-identification and then turn to Landi that de-identifies i) by a different method and ii) in a method not compatible with HIPAA.

D. Analysis of Ground 4: the Dick-Landi-Murphy Combination Fails to Render the Challenged Claims Obvious

1. Analysis

199. The Petition relies on Murphy for elements [1.e], [5], [11], [12], [14.e], and [18]. Pet., 68–74. In analyzing claim 11, the Petition merely provides the following terse explanation¹¹:

Murphy makes clear that, in complying with HIPAA, an algorithm preferably blocks queries that return fewer than 3 patients to prevent the user from associating the patient with a particular record. Ex. 1009, 555. (“[W]e modify our range algorithm to have a wider obfuscation at values close to zero, and indicate the greater range by returning ‘<3’ when the obfuscated number is less than 3.”); Ex. 1003, ¶242. Ensuring a minimum number of tokens are identified would have been a simple design choice to comply with HIPAA. Ex. 1003, ¶¶66, 239-40.

Pet., 69.

200. The Petition’s analysis is problematic for multiple reasons and fails to show that the Dick-Landi-Murphy combination would have rendered obvious the features of the above-listed claim elements.

¹¹ The Petition simply cites back to this same discussion from claim 11 without more when mapping the additional features recited in each of [1.e], [5], [12], [14.e], and [18]. Pet., 68–71. Notably, the Petition fails to address any of the differences in claim scope between these elements or explain how Murphy meets the specific limitations recited in each element.

201. First, the Petition’s assertion that Murphy’s algorithm “blocks queries” when the number of patients is less than 3 is incorrect. For results around zero, Murphy teaches modifying the “range algorithm to have a wider obfuscation at values close to zero, and [indicating] the greater range by returning ‘<3’ when the obfuscated number is less [than] 3.” EX1009, 555. Widening the obfuscation range in these cases is far different from blocking a query as alleged. To the contrary, the query tool always returns a numerical result to the query by applying an obfuscation algorithm. The obfuscation algorithm for results less than three involves providing an indication that the obfuscated result is less than three, rather than returning an absolute value or no value at all. The query is still answered, however, as the result informs the requester that the number of matching patients is near zero, and even this result bears a relationship to the true number of patients identified in response to the request. Importantly, Murphy’s query tool does not return actual patient records, but instead returns numerical values. *Id.* So, any numerical result, including ‘<3,’ constitutes a response to the query. *Id.* Accordingly, Murphy does not teach “blocking queries,” as argued by the Petition.

202. Second, the fact that Murphy’s query tool returns an “obfuscated” number of patients and makes its decision whether to apply wider obfuscation based on whether the “*obfuscated number* is less than 3” means that Murphy does not operate based on “a minimum number of individuals” or a “minimum number

of corresponding tokens” as claimed. The claims relate to a minimum number of individuals in the group or in the corresponding tokens—not “obfuscated” numbers as described in Murphy. Even if Murphy did “block queries” when there are fewer than a certain number of patients in the obfuscated result (which it does not), the decision whether to block such queries would be based on some obfuscated number of patients rather than the number of individuals in the group or a minimum number of corresponding tokens as claimed. Thus, Murphy is simply inapplicable to the claimed features.

203. Finally, the Petition has not established that it would be obvious to combine Murphy’s teachings with the system of Dick and Landi. Dick and Landi each describe systems that involve de-identifying patient data and making that de-identified data accessible to researchers and other interested users. *Supra*, §VIII.D–E. Murphy does no such thing. Murphy explicitly considered and rejected the option of “de-identify[ing] patients in the database.” Murphy also rejects techniques where the patient information is susceptible to re-identification, like in Landi. EX1009, 553. Instead, Murphy opted to provide a query tool that would merely respond with a simple, obfuscated number of patients that match the search criteria without ever returning de-identified health records. Murphy’s obfuscation of the number of patients returned by a query tool in this context is completely different from Dick and Landi, and it would not have been obvious to

condition the processes or results of Dick and Landi based on Murphy's teachings in this regard.

204. Therefore, and for each of these reasons, challenged claims are patentable over the Dick-Landi-Murphy combination.

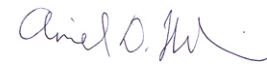
X. CONCLUSION

205. For the foregoing reasons, I disagree with each ground presented in the Petition. Accordingly, it is my opinion that Petition fails to demonstrate that any claim of the '641 patent is invalid.

206. I currently hold the opinions set expressed in this declaration. But my analysis may continue, and I may acquire additional information and/or attain supplemental insights that may result in added observations.

207. 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 the Title 18 of the United States Code.

Executed this 7th Day of October, 2024.



Aviel D. Rubin

APPENDIX A

Aviel D. Rubin, Ph.D.

Professor Emeritus, Johns Hopkins University
Founder & Managing Partner, Harbor Experts

avirubin@gmail.com

<https://www.linkedin.com/in/avirubin/>



Overview

Avi Rubin is a Computer Scientist with almost a decade of industry experience followed by over 20 years in academia. After receiving his Ph.D. in Computer Science from the University of Michigan in 1994, Dr. Rubin worked as a researcher at Bellcore and then at AT&T Labs. In 2003, he joined the Computer Science faculty at Johns Hopkins University and was promoted to Full Professor with Tenure in 2004. During his over 20 years at Johns Hopkins, Dr. Rubin was Technical Director of the JHU Information Security Institute, along with his regular faculty position. In 2023, he was appointed Computer Science Professor Emeritus at Johns Hopkins. Dr. Rubin is a frequent keynote speaker at industry and academic conferences and delivered widely viewed TED talks in 2011 and 2015. He has testified about information and network security before Congress on multiple occasions and frequently testifies as an expert witness in Federal court. His awards include Fulbright Scholar, Baltimorean of the Year, and the EFF Pioneer Award.

Academic Degrees

- 1994, **Ph.D.**, Computer Science and Engineering, University of Michigan, Ann Arbor
- 1991, **M.S.E.**, Computer Science and Engineering, University of Michigan, Ann Arbor
- 1989, **B.S.**, Computer Science (Honors), University of Michigan, Ann Arbor

Academic Appointments

September, 2023 - present

Professor Emeritus, Johns Hopkins University

April, 2004 - August, 2023

Professor (with tenure), Johns Hopkins University

August, 2010 - July, 2011

Visiting Research Professor, Fulbright Scholar, Tel Aviv University, Israel

January, 2003 - April, 2004

Associate Professor, Johns Hopkins University

January, 2003 - August, 2023

Technical Director, Johns Hopkins University Information Security Institute

2006 - 2010

Director and Principal Investigator (PI), NSF ACCURATE Center

1995 - 1999

Adjunct Professor, New York University

Summer, 1999

Visiting Professor, École Normale Supérieure, Paris, France

1988 - 1993

Teaching Assistant, University of Michigan

Doctoral Committees

Doctoral Thesis Advisor: David Inyangson, JHU

Doctoral Thesis Advisor: Logan Kostick, JHU

Doctoral Thesis Advisor: Atheer Almogbil, JHU (May, 2024)

Doctoral Thesis Advisor: Tushar Jois, JHU (May, 2023)

Doctoral Thesis Advisor: Random Gwinn, JHU (May, 2022)

Doctoral Thesis Advisor: Karl Siil, JHU (May, 2022)

Doctoral Thesis Advisor: James Cervini, JHU (May, 2022)

Doctoral Thesis Advisor: Jeff Chavis, JHU (May, 2021)

Doctoral Thesis Advisor: Gabe Kaptchuk, JHU (May, 2020)

Dissertation Committee: Thomas Tantillo, JHU (September, 2018)

Doctoral Thesis Advisor: Paul Martin, JHU (February, 2016)

Doctoral Thesis Advisor: Michael Rushanan, JHU (May, 2016)

Doctoral Thesis Advisor: Ayo Akinyele, JHU (December, 2013)

Doctoral Thesis Advisor: Matthew Pagano, JHU (August, 2013)

Doctoral Thesis Advisor: Ryan Gardner, JHU (August, 2009)

Doctoral Thesis Advisor: Sam Small, JHU (May, 2009)

Doctoral Thesis Advisor: Sujata Doshi, JHU (May, 2009)

Doctoral Thesis Advisor: Joshua Mason, JHU (June, 2009).

Dissertation Committee: J. Alex Halderman, Princeton University (May, 2009).

Dissertation Committee: Sophie Qiu (May, 2007).

Doctoral Thesis Advisor: Adam Stubblefield (April, 2005).

Dissertation Committee: Kevin FU, MIT (February, 2005).

Dissertation Committee: Robert Fischer, Harvard University (June, 2003).

Dissertation Committee: Marc Waldman, New York University, (April, 2003).

Dissertation Committee: Patrick McDaniel, U. of Michigan (September, 2001).

Doctoral Thesis Advisor: Fabian Monrose, New York University (April, 1999).

Dissertation Committee: Mike Just, Carleton University (November, 1998).

Dissertation Committee: Trent Jaeger, University of Michigan (October, 1996).

Industry Experience

2011 - present

Harbor Labs, Founder & Chief Scientist

2005 - 2011

Independent Security Evaluators, Founder & President

1997 - 2002

AT&T Labs -- Research, Secure Systems Research Department

1994 - 1996

Bellcore, Cryptography and Network Security Research Group

Summer, 1990

Great Lakes Software Co., Programmer, Howell, MI

Summer, 1989

IBM, Programmer, Meyers Corners Lab, Poughkeepsie, NY

Books

- Aviel D. Rubin, *Brave New Ballot*, Random House, (September, 2006).
- William R. Cheswick, Steven M. Bellovin and Aviel D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker (2e)*, Addison Wesley Publishing Company, Inc., (February, 2003).
- **Chapter 4**, *Communications Policy and Information Technology: Promises, Problems, Prospects*, MIT Press, Lorrie Faith Cranor and Shane Mitchell Greenstein, eds., (2002).
- Aviel D. Rubin, *Whitehat Security Arsenal*, Addison Wesley Publishing Company, Inc., (June, 2001).
- **Chapter 8**, Publius and **Chapter 14**, Trust in Distributed Systems, Marc Waldman, Lorrie Faith Cranor, and Aviel D. Rubin, *PeertoPeer*, O'Reilly & Associates, Inc., (February, 2001).
- Aviel D. Rubin, Daniel Geer, Marcus J. Ranum, *Web Security Sourcebook*, John Wiley & Sons, Inc., (June, 1997).
- **Ph.D. dissertation**: *Nonmonotonic Cryptographic Protocols*, University of Michigan, Ann Arbor (April, 1994).

Refereed Journal Publications

- David Kotz, Kevin Fu, Carl Gunter, Avi Rubin, *Security for Mobile and Cloud Frontiers in Healthcare*, Communications of the ACM (July, 2015).
- Ayo Akinyele, Christina Garman, Matthew D. Green, Ian Miers, Matthew Pagano, Aviel D. Rubin, Michael Rushanan, *Charm: A Framework for Rapidly Prototyping Cryptosystems*, Journal of Cryptographic Engineering (JCEN), (January, 2013).
- Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *Detecting Code Alteration by Creating a Temporary Memory Bottleneck*, IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, (December, 2009).
- Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, Avi Rubin, *Anonymity in Wireless Broadcast Networks*, International Journal of Network Security (IJNS), (January, 2008).
- Stephen Bono, Aviel Rubin, Adam Stubblefield, and Matthew Green, *Security Through Legality*, Communications of the ACM (June, 2006).
- Adam Stubblefield, Dan S. Wallach, and Aviel D. Rubin, *Managing the Performance Impact of Web Security*, Electronic Commerce Research Journal, February, 2005.
- David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, *Analyzing Internet Voting Security*, Communications of the ACM (October, 2004).
- Simon Byers, Aviel D. Rubin, and David Kormann, *Defending Against an Internet-based Attack on the Physical World*, ACM Transactions on Internet Technology (TOIT), August, 2004.
- Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)* ACM Transactions on Information and System Security, May, 2004.

- Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, Communications of the ACM (December, 2002).
- Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *The Architecture of Robust Publishing Systems*, ACM Transactions on Internet Technology (TOIT), (November, 2001).
- David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single-Signon Protocol*, Computer Networks, (July, 2000).
- Christian Gilmore, David P. Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, IEEE Network, (November, 1999).
- Fabian Monroe and Aviel D. Rubin, *Keystroke Dynamics as a Biometric for Authentication*, Future Generation Computer Systems, (March, 2000).
- Michael K. Reiter and Aviel D. Rubin, *Anonymity Loves Company: Anonymous Web Transactions with Crowds*, Communications of the ACM (February, 1999).
- Aviel D. Rubin and Daniel E. Geer, Jr., *Mobile Code Security*, IEEE Internet Computing (November/December, 1998).
- Aviel D. Rubin and Daniel E. Geer, Jr., *A Survey of Web Security*, IEEE Computer, (September, 1998).
- Michael K. Reiter and Aviel D. Rubin, *Crowds: Anonymity for Web Transactions*, ACM Transactions on Information and System Security, (June, 1998).
- Aviel D. Rubin, *An Experience Teaching a Graduate Course in Cryptography*, Cryptologia (April, 1997).
- Aviel D. Rubin, *Extending NCP for public Key Protocols*, Mobile Networks and Applications (ACM/Balzer), 2(3) (April, 1997).
- Aviel D. Rubin, *Independent One-Time Passwords*, USENIX Journal of Computer Systems (February, 1996).
- Aviel D. Rubin, *Secure Distribution of Documents in a Hostile Environment*, Computer Communications (June, 1995).

Refereed Conference Publications

- Tushar Jois, Gabrielle Beck, Sofia Belikovetsky, Joseph Carrigan, Alishah Chator, Logan Kostick, Maximilian Zinkus, Gabriel Kaptchuk, Aviel D. Rubin, *SocloTy: Practical Cryptography in Smart Home Contexts*, Privacy Enhancing Technologies Symposium 2024 (PETS '24), (July, 2024).
- Atheer Almogbil , Momo Steele , Sofia Belikovetsky , Adil Inam, Olivia Wu, Aviel Rubin, Adam Bates, *Using Behavior Monitoring to Identify Privacy Concerns in Smarthome Environments*, NDSS Workshop on Security and Privacy in Standardized IoT (SDIoTSec), (February, 2024).
- Samra Kasim, Nawal Valliani, Nelson Ka Ki Wong, Shahin Samadi, Lanier Watkins and Aviel Rubin, *Explainable Autonomic Cybersecurity for Industrial Control Systems*, IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), (March, 2023).
- Valeti Manoj, Shao Wenda, Niu Sihan, Christopher Rouff, Lanier Watkins, Aviel Rubin, *Cybersecurity as a Tic-Tac-Toe Game Using Autonomous Forwards (Attacking) And Backwards (Defending) Penetration Testing in a Cyber Adversarial Artificial Intelligence System*, IEEE International Conference of Computer Science and Information Technology (ICOSNIKOM),(October, 2022).

- James Cervini & Aviel D. Rubin, *Don't Drink the Cyber: Extrapolating the Possibilities of Oldsmar's Water Treatment Cyberattack*, ICCWS 17th International Conference on Cyber Warfare and Security, (July, 2022).
- Gabriel Kaptchuk, Tushar Jois, Matthew Green, Aviel Rubin, *Make Steganography Great Again — Before It's Too Late*, Real World Crypto 2022, (April, 2022).
- James Cervini, Daniel Muller, Alexander Beall, Joseph Maurio, Aviel Rubin & Lanier Watkins, *A Backfit Approach for Trusted Virtualization-Based Programmable Logic Controller Resilience*, Sixteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, (March, 2022).
- Hedin Beattie, Lanier Watkins, William H. Robinson, Aviel Rubin, Shari Watkins, *Measuring and Mitigating Bias in AI-Chatbots*, 2022 IEEE International Conference on Assured Autonomy (ICAA'22), (March, 2022).
- Random Gwinn, Mark Matties, Aviel D. Rubin, *Wavelet Selection and Employment for Side-Channel Disassembly*, IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE), (December, 2021).
- Karl A Siil, Aviel D. Rubin, Matthew C. Elder, Anton T Dahbura, Matthew Green, Lanier Watkins, *Cost-Effective Mission Assurance Engineering Through Simulation*, The 2021 International Conference on Internet of Things and Intelligence Systems (IoTIS'21), (November, 2021).
- Gabriel Kaptchuk, Tushar Jois, Matthew Green, Aviel Rubin, *Meteor: Cryptographically Secure Steganography for Realistic Distributions*, 28th ACM Conference on Computer and Communications Security (CCS '21), (November, 2021).
- James Schaffter, Aviel Rubin and Lanier Watkins, *A Containerization-Based Backfit Approach for Industrial Control System Resiliency*, SafeThings '21 Workshop, (May, 2021).
- Tushar Jois, Claudia Moncaliano, Khir Henderson, Aviel D. Rubin, *WDPKR: Wireless Device Profiling Kit and Reconnaissance*, 2021 Hot Topics in the Science of Security (HotSoS) Symposium (April, 2021).
- Lanier Watkins, ChangHao Cho, John Hurley, Aviel D. Rubin, *Collaborative Global Impact Cloud Computing Risk Assessment Framework*, International IoT, Electronics and Mechatronics Conference (IEMTRONICS '21), (April, 2021).
- Jeffrey S. Chavis, Malcom Doster, Michelle Feng, Syeda Zeeshan, Samantha Fu, Elizabeth Aguirre, Antonio Davila, Kofi Nyarko, Aaron Kunz, Tracy Herriotts, Daniel Syed, Lanier Watkins, Anna Buczak, Aviel Rubin, *A Voice Assistant for IoT Cybersecurity*, Integrated STEM Education Conference (ISEC '21), (March, 2021).
- Lanier Watkins, Danzel Hamilton, Kevin Kornegay, Aviel Rubin, *Triaging Autonomous Drone Faults by Simultaneously Assuring Autonomy and Security in Autonomous Drones*, 55th Annual Conference on Information Sciences and Systems (CISS '21), (March, 2021).
- Lanier Watkins, James Ballard, Kevin Hamilton, William H. Robinson, Aviel Rubin, Cleon Davis, *Bio-Inspired, Host-based Firewall* (Refereed WIP paper), 23rd IEEE International Conference on Computational Science and Engineering (CSE), (December, 2020).
- Lanier Watkins, Yue Yu, Sifan Li, William H. Robinson, Aviel D. Rubin, *Using Deep Learning to Identify Security Risks of Personal Mobile Devices in Enterprise Networks*, The 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), (October, 2020).

- Lanier Watkins, Kevin D. Fairbanks, Chengyu Li, Mengdi Yang, William H. Robinson, Aviel D. Rubin, *A Black Box Approach to Inferring Characterizing, and Breaking Native Device Tracking Autonomy*, The 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), (October, 2020).
- Karl Siil, Aviel Rubin, Matthew Elder, Anton Dahbura, Matthew Green, Lanier Watkins, *Mission Assurance for Autonomous Undersea Vehicles*, IEEE Workshop on Assured Autonomous Systems (WAAS), (May, 2020).
- Jeffrey Chavis, Aaron Kunz, Lanier Watkins, Anna Buczak, Aviel Rubin, *A Capability for Autonomous IoT System Security: Pushing IoT Assurance to the Edge*, IEEE Workshop on Assured Autonomous Systems (WAAS), (May, 2020).
- Lanier Watkins, Shane Sartalamacchia, Richard Bradt, Karan Dhareshwar, Harsimar Bagga, William H. Robinson, Aviel Rubin, *Defending Against Consumer Drone Privacy Attacks: A Blueprint For A Counter Autonomous Drone Tool*, ISOC Workshop on Decentralized IoT Systems and Security (DISS 2020), (February, 2020).
- Adrian Cartagena, Gerald Rimmer, Thomas Van Dalsen, Lanier Watkins, William H. Robinson, Aviel D. Rubin, *Privacy Violating Opensource Intelligence Threat Evaluation Framework: A Security Assessment Framework for Critical Infrastructure Owners*, 10th Annual Computing and Communications Workshop and Conference (IEEE CCWC 2020), (January, 2020).
- Jeffrey Chavis, Lanier Watkins, Anna Buczak, Aviel D. Rubin, *Connected Home Automated Security Monitor (CHASM): Protecting IoT Through Application of Machine Learning*, 10th Annual Computing and Communications Workshop and Conference (IEEE CCWC 2020), (January, 2020).
- Lanier Watkins, Shreya Aggarwal, Omotola Akeredolu, William H. Robinson and Aviel D. Rubin, *Tattle Tail Security: An Intrusion Detection System for Medical Body Area Networks*, Workshop on Decentralized IoT Systems and Security (DISS '19), (February, 2019).
- Lanier Watkins, Juan Ramon, Gaetano Snow, Jessica Vallejo, William H. Robinson, Aviel D. Rubin, Joshua Ciocco, Felix Jedrzejewski, Jinglun Liu, Chengyu Li, *Exploiting Multi-Vendor Vulnerabilities as BackDoors to Counter the Threat of Rogue Small Unmanned Aerial Systems*, ACM Workshop on Mobile IoT Sensing, Security, and Privacy (Mobile IoT SSP '18), (June, 2018).
- Paul D. Martin, David Russel, Malek Ben Salem, Stephen Checkoway, Aviel D. Rubin, *Sentinel: Secure Mode Profiling and Enforcement for Embedded Systems*, Proc. ACM/IEEE International Conference on Internet-of-Things Design and Implementation, (April, 2018).
- Gabriel Kaptchuk, Matthew D. Green and Aviel D. Rubin, *Outsourcing Medical Dataset Analysis: A Possible Solution*, Financial Cryptography Conference, (April, 2017).
- Michael Rushanan, David Russell and Aviel D. Rubin, *Mallory-Worker: Stealthy Computation and Covert Channels using Web Workers*, Proceedings of the 12th International Workshop on Security and Trust Management, (September, 2016).
- Paul Martin, Michael Rushanan, Thomas Tantillo, Christoph Lehmann and Aviel Rubin, *Applications of Secure Location Sensing in Healthcare*, Proceedings of the 7th ACM Conference on Bioinformatics, Computational Biology, and Health Informatics, (October, 2016).

- Gabriel Kaptchuk and Aviel D. Rubin, *A Practical Implementation of a Multi-Device Split Application for Protecting Online Poker*, Proceedings of the 15th Annual Security Conference, (March, 2016).
- Aviel D. Rubin, *Taking Two-Factor to the Next Level: Protecting Online Poker, Banking, Healthcare and Other Applications*, Proceedings of the 2014 Annual Computer Security Applications Conference, Invited Keynote Essay, (December, 2014).
- Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson, *Security and Privacy in Implantable Medical Devices and Body Area Networks*, IEEE Symposium on Security and Privacy-SoK Track (May, 2014).
- Christina Garman, Matthew Green, Ian Miers, Aviel D. Rubin, *Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity*, 1st Workshop on Bitcoin Research (March, 2014).
- Paul Martin, Aviel Rubin and Rafae Bhatti, *Enforcing Minimum Necessary Access in Healthcare Through Integrated Audit and Access Control*, Health Informatics Symposium at the ACM Conference on Bioinformatics, Computational Biology, and Biomedical Informatics, (September, 2013).
- Ian M. Miers, Christina Garman, Matthew D. Green, Aviel D. Rubin, *Zerocoin: Anonymous Distributed e-Cash from Bitcoin*, Proc. IEEE Symposium on Security and Privacy (May, 2013).
- Ian M. Miers, Matthew D. Green, Christoph U. Lehmann, Aviel D. Rubin, *Vis-à-Vis Cryptography: Private and Trustworthy In-Person Certifications*, In Proceedings of the 3rd USENIX/HealthSec Workshop, (August, 2012).
- Joseph A. Akinyele, Matthew W. Pagano, Matthew D. Green, Christoph U. Lehmann, Zachary N. J. Peterson and Aviel D. Rubin, *Securing Electronic Medical Records Using Attribute-Based Encryption On Mobile Devices*, ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, (October, 2011).
- Matthew D. Green, Aviel D. Rubin, *A Research Roadmap for Healthcare IT Security inspired by the PCAST Health Information Technology Report 4-page Extended Abstract*, In Proceedings of the 2nd USENIX/HealthSec Workshop, (August, 2011).
- Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Designing for Audit: A Voting Machine with a Tiny TCB*, Financial Cryptography Conference, (January, 2010).
- Ryan Gardner, Sujata Garera, Matthew W. Pagano, Matthew D. Green, Aviel D. Rubin, *Securing Medical Records on Smart Phones*, Workshop on Security and Privacy in Medical and Home-Care Systems, (November, 2009).
- Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Coercion Resistant End-to-end Voting*, Financial Cryptography Conference, (February, 2009).
- Ryan Gardner, Sujata Garera, Anand Rajan, Carols Rozas, Aviel D. Rubin, Manoj Sastry, *Protecting Patient Records from Unwarranted Access*, Future of Trust in Computing, (July, 2008).
- Sujata Garera, Niels Provos, Monica Chew and Aviel D. Rubin, *A Framework for Detection and Measurement of Phishing Attacks*, 5th ACM Workshop on Recurring Malcode (WORM '07), (November, 2007).
- Sujata Garera and Aviel D. Rubin, *An Independent Audit Framework for Software Dependent Voting Systems*, 14th ACM Conference on Computer and Communications Security, (November, 2007).

- Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *On the Difficulty of Validating Voting Machine Software with Software*, In Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07), (August, 2007).
- Sujata Doshi, Fabian Monrose, and Aviel D. Rubin, *Efficient Memory Bound Puzzles using Pattern Databases*, 4th International Conference on Applied Cryptography and Network Security (ACNS'06), (June, 2006).
- Sophie Qiu, Patrick McDaniel, Fabian Monrose, and Aviel Rubin, *Characterizing Address Use Structure and Stability of Origin Advertisement in Interdomain Routing*, 11th IEEE Symposium on Computers and Communications, (June 2006).
- Zachary Peterson, Randal Burns, Joseph Herring, Adam Stubblefield, and Aviel D. Rubin, *Secure Deletion for a Versioning Filesystem*, Proc. USENIX Conference on File and Storage Technologies (FAST '05), (December, 2005).
- Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin, Michael Szydlo, *Security Analysis of a Cryptographically-Enabled RFID Device*, 14th USENIX Security Symposium, (August, 2005).
- Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System*, Proc. IEEE Symposium on Security and Privacy (May, 2004).
- Nathanael Paul, David Evans, Aviel D. Rubin and Dan Wallach, *Authentication for Remote Voting*, ACM Workshop on Human-Computer Interaction and Security Systems (April, 2003).
- Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Aviel Rubin, *Protocols for Anonymity in Wireless Networks*, Proc. 11th International Workshop on Security Protocols (April, 2003).
- Geoffrey Goodell, William Aiello, Timothy Griffin, John Ioannidis, Patrick McDaniel, Aviel Rubin, *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing*, Proc. ISOC Symposium on Network and Distributed System Security (February, 2003).
- Simon Byers, Aviel D. Rubin, David Kormann, *Defending Against an Internet-based Attack on the Physical World*, ACM Workshop on Privacy in the Electronic Society (November, 2002).
- Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, Proc. ISOC Symposium on Network and Distributed System Security (February, 2002).
- Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, 29th Research Conference on Communication, Information and Internet Policy (TPRC2001), (October, 2001).
- Aviel D. Rubin and Rebecca N. Wright, *Offline generation of limited-use credit card numbers*, Financial Cryptography Conference, (February, 2001).
- Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *Publius, A robust, tamper-evident and censorship-resistant web publishing system*, 9th USENIX Security Symposium, (August, 2000).
- David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single Sign-on Protocol*, 9th International World Wide Web Conference, (May, 2000).
- Patrick McDaniel and Aviel D. Rubin, *A Response to "Can we Eliminate Certificate Revocation Lists?"*, Financial Cryptography Conference, (February, 2000).

- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, *Using smartcards to secure a personalized gambling device*, 6th ACM Conference on Computer and Communications Security, (November, 1999).
- Ian Jermyn, Alain Mayer, Fabian Monroe, Michael K. Reiter, and Aviel D. Rubin, *The Design and Analysis of Graphical Passwords*, 8th USENIX Security Symposium, (August, 1999).
- Christian Gilmore, David Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Fabian Monroe, Peter Wykoff, and Aviel D. Rubin, *Distributed Execution with Remote Audit*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Dahlia Malkhi, Michael K. Reiter and Aviel D. Rubin, *Secure Execution of Java Applets using a Remote Playground*, Proc. IEEE Symposium on Security and Privacy (May, 1998).
- Aviel D. Rubin, Dan Boneh, and Kevin Fu, *Revocation of Unread Email in an Untrusted Network*, Second Australasian Conference on Information Security and Privacy (July, 1997).
- Fabian Monroe and Aviel D. Rubin, *Authentication via Keystroke Dynamics*, 4th ACM Conference on Computer and Communications Security (April, 1997).
- David M. Martin, Siviramakrishnan Rajagopalan, and Aviel D. Rubin, *Blocking Java Applets at the Firewall*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1997).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *A System Architecture for Flexible Control of Downloaded Executable Content*, 5th International Workshop on Object-Orientation in Operating Systems (October, 1996).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *Building Systems that Flexibly Control Downloaded Executable Content*, Proc. 6th USENIX Security Symposium (July, 1996).
- Victor Shoup and Aviel D. Rubin, *Session Key Distribution Using Smart Cards*, Proc. of Eurocrypt '96 (May, 1996).
- Trent Jaeger & Aviel D. Rubin, *Preserving Integrity in Remote File Location and Retrieval*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1996).
- Aviel D. Rubin, *Extending NCP for Public Key Protocols*, Proc. IEEE 4th International Conference on Computer Communications and Networks (September, 1995).
- Aviel D. Rubin, *PseudoRandom Functions for OneTime Passwords*, Proc. 5th USENIX UNIX Security Symposium (June, 1995).
- Aviel D. Rubin, *Trusted Distribution of Software Over the Internet*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1995).
- Aviel D. Rubin & Peter Honeyman, *Nonmonotonic Cryptographic Protocols*, Proc. IEEE Computer Security Foundations Workshop VII (June, 1994).
- Aviel D. Rubin & Peter Honeyman, *Long Running Jobs in an Authenticated Environment*, Proc. 4th USENIX UNIX Security Symposium (October, 1993).

Patents

- Aviel D. Rubin, "Broadband Certified Mail", **US Patent Numbers 6,990,581**, (January 24, 2006) and 9,876,769, (January 23, 2018).

- Aviel D. Rubin, Utilization of multiple devices to secure online transactions, **US Patent Number 9,064,376**, (June 23, 2015).
- Steven M. Bellovin, Thomas J. Killian, Bruce LaRose, Aviel D. Rubin, Norman L. Schryer, Method and apparatus for connection to virtual private networks for secure transactions, **US Patent Numbers 8,239,531**, (August 7, 2012) and **8,676,916** (March 18, 2014).
- Christian A. Gilmore, David P. Kormann, and Aviel D. Rubin, Method and apparatus for secure remote access to an internal web server, **US Patent Number 7,334,126**, (February 19, 2008).
- Aviel D. Rubin, "Method for secure remote backup", **US Patent Number 7,222,233**, (May 22, 2007).
- Frederick Douglass, Michael Rabinovich, Aviel D. Rubin, and Oliver Spatscheck, "Method for content distribution in a network supporting a security protocol", **US Patent Number 7,149,803**, (December 12, 2006).
- William A. Aiello, Steven M. Bellovin, Charles Robert Kalmanek, Jr., William T. Marshall, and Aviel D. Rubin, "Method and apparatus for enhanced security in a broadband telephony network", **US Patent Number 7,035,410**, (April 25, 2006).
- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, "Using smartcards to enable probabilistic transaction on an untrusted device", **US Patent Number 6,496,808**, (December 17, 2002).
- Aviel D. Rubin and Victor J. Shoup, "Session Key Distribution Using Smart Cards", **US Patent Number 5,809,140**, (September 15, 1998).
- Aviel D. Rubin, "Method for the Secure Distribution of Electronic Files in a Distributed Environment", **US Patent Number 5,638,446**, (June 10, 1997).

Professional Activities

Board of Directors

Director, Maryland Israel Development Center (MIDC), (2013-2018).

Director, USENIX Organization, elected by popular vote (2000-2004).

Editorial and Committees

Chair: IEEE Security & Privacy Symposium Test of Time Awards Committee for 2008-2010 Conferences, May, 2020.

Associate Editor: IEEE Transactions on Information Forensics and Security (2009 - 2011).

Associate Editor: Communications of the ACM (CACM), 2009 - 2017.

Guest Co-Editor: IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, December 1, 2009.

Guest Co-Editor: IEEE Security & Privacy Magazine, Special Issue on Electronic Voting, October/November, 2007.

Associate Editor: IEEE Transactions on Software Engineering (2005-2006). Editorial and

Advisory Board: International Journal of Information and Computer Security (IJICS) (2004 - 2006).

Guest Co-Editor: IEEE Computer Networks, Special Issue on Web Security, January, 2005.

Editorial Board: Journal of Privacy Technology (2004-2006).

Guest Co-Editor: IEEE Security & Privacy Magazine, Special Issue on Electronic Voting Security, January/February, 2004.

Member: Security Peer Review Group (SPRG) of the Federal Voting Assistance Program's (FVAP) Secure Electronic Registration and Voting Experiment (SERVE) Project, 2003 - 2004.

Member: DARPA Information Science And Technology Study Group (2003 - 2006).

Associate Editor: IEEE Security & Privacy Magazine (2003 - 2011).

Guest Editor: Communications of the ACM, Special Issue on Wireless Networking Security, May, 2003.

Associate Editor: ACM Transactions on Internet Technology (2002-2005).

Executive Committee Member: DIMACS Workshop Series with Special Focus on Network Security (2002 - 2004).

Advisory Board Member: Information Security and Cryptography Book Series, Springer, 2001- 2006.

Member: Steering Group, ISOC Symposium on Network and Distributed System Security, 2001 - 2004.

Member: Government Infosec Science and Technology Study Group on malicious code, 1999 - 2000.

Member: AT&T Internet Intellectual Property Review Team, 1999 - 2001. Associate Editor: Electronic Commerce Research Journal, Baltzer Science Publishers, 1999 - 2002.

CoEditor: Electronic Newsletter of the IEEE Technical Committee on Security & Privacy, with Paul Syverson, 1998.

Editorial Board: Bellcore Security Update Newsletter, 1995 - 1996.

Conference Committees

- **Program Committee member:** NDSS Workshop: Innovative Secure IT Technologies Against COVID19, San Diego, CA, February, 2020.
- **Program Committee member:** Financial Cryptography '15 Barbados, February, 2015.
- **Program Committee member:** USENIX HealthTech Workshop on Health Information Technologies (HealthTech '15), August 11, 2015.
- **Program Co-chair:** (w/Eugene Vasserman) USENIX HealthTech Workshop on Health Information Technologies (HealthTech '14), August 19, 2014.
- **Program committee member:** 2nd USENIX Workshop on Health Security & Privacy (HealthSec '11), August 9, 2011.
- **Program Co-chair:** (w/Kevin Fu & Yoshi Kohno), 1st USENIX Workshop on Health Security and Privacy (HealthSec '10), August 10, 2010.
- **Program Committee member:** First Security and Privacy in Medical and HomeCare Systems Workshop (SPIMACS), Chicago, IL, November 13, 2009.
- **Invited Talks Co-Coordinator:** 17th USENIX Security Symposium, San Jose, CA, July 28 August 1, 2008.
- **Program Co-chair:** (w/Patrick McDaniel): IEEE Symposium on Security and Privacy, Oakland, California, May 18-22, 2008.
- **Program Co-chair:** (w/Giovani Di Crescenzo): Financial Cryptography '06 Anguilla BWI, February, 2006.
- **Program Committee member:** IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 2004.
- **Program Committee member:** Financial Cryptography '04 Key West, Florida, February 9-12, 2004.

- **Program Committee member:** 2nd ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., October 30, 2003.
- **Program Committee member:** 10th ACM Conference on Computer and Communications Security, Washington D.C., October 27-30, 2003.
- **Program Committee member:** 8th European Symposium on Research in Computer Science (ESORICS), Norway, October 13-15, 2002.
- **Program Vice Chair:** Security and Privacy Track, The Twelfth International World Wide Web Conference, Budapest, Hungary, May 2004, 2003.
- **Program Committee member:** IEEE Symposium on Security and Privacy, Oakland, California, May 11-14, 2003.
- **Program Committee member:** Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.
- **Program Committee member:** 4th International Conference on Information and Communications Security (ICICS), Kent Ridge Digital Labs (KRDL), Singapore December 9-12, 2002.
- **Program Committee member:** ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., November 21, 2002.
- **Program Committee member:** 9th ACM Conference on Computer and Communications Security, Washington D.C., November 17-21, 2002.
- **Program Committee member:** 5th International Conference on Electronic Commerce Research (ICECR5), Montreal, Canada, October 23-27, 2002.
- **Program Committee member:** 2nd Symposium on Requirements Engineering for Information Security (SREIS), Raleigh, North Carolina, Oct 14-15, 2002.
- **Program Committee member:** 7th European Symposium on Research in Computer Science (ESORICS), Zurich, Switzerland, October 14-16, 2002.
- **Program Committee member:** 11th USENIX Security Symposium, San Francisco, Ca, August 5-9, 2002.
- **Program Committee member:** International Workshop on Global and Peer-to-Peer Computing at IEEE International Symposium on Cluster Computing and the Grid (CCGrid'2002), Berlin, Germany, May 21-24, 2002.
- **Program Committee member:** 11th International World Wide Web Conference Honolulu, Hawaii, May 7-11, 2002.
- **Program Committee member:** 2nd Workshop on Privacy Enhancing Technologies San Francisco, CA, April 14-15, 2002.
- **Program Committee member:** The 1st International Workshop on Peer-to-Peer Systems (IPTPS'02) MIT Faculty Club, Cambridge, MA, March 78, 2002.
- **Program Committee member:** The 4th International Conference on Telecommunications and Electronic Commerce Dallas, TX, November, 2001. **Program Committee member:** 10th USENIX Security Symposium, Washington D.C., August 13-17, 2001.
- **Program Committee member:** Financial Cryptography '01 Grand Cayman, Cayman Islands, BWI, February, 2001.
- **Program Co-chair:** (w/Paul Van Oorschot): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 7-9, 2001.
- **Program Committee member:** The 3rd International Conference on Telecommunications and Electronic Commerce Dallas, TX, November 16-19, 2000. **Program Committee member:** 9th USENIX Security Symposium, Denver, Colorado, August 14-17, 2000.

- **Program Committee member:** Workshop on Design Issues in Anonymity and Unobservability Berkeley, California, July 2526, 2000.
- **Program Committee member:** Performance and Architecture of Web Servers (PAWS), Santa Clara, CA, June 18, 2000.
- **Program Co-chair:** (w/Gene Tsudik): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 24, 2000.
- **Program Committee member:** 1999 International Information Security Workshop (ISW'99), Kuala Lumpur, Malaysia, November 67, 1999.
- **Program Committee member:** 2nd Int'l. Conference on Telecommunications and Electronic Commerce, Nashville, TN, October 68, 1999.
- **Invited Talks coordinator:** 8th USENIX Security Symposium, Washington D.C., August, 1999.
- **Program Chair:** 24th USENIX Annual Technical Conference, Monterey, CA, June 711, 1999.
- **Program Committee member:** 8th International World Wide Web Conference , Toronto, Canada, May 1114, 1999.
- **Program Committee member:** 3rd USENIX workshop on Electronic Commerce , Boston, MA, August 31 September 3, 1998.
- **Program Committee member:** 5th ACM Conference on Computer and Communications Security, San Francisco, CA, November 35, 1998.
- **Program Chair:** 7th USENIX Security Symposium, San Antonio, TX, Jan. 2629, 1998.
- **Program Committee member:** 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 24, 1997.
- **Program Committee member:** 6th USENIX Security Symposium, San Jose, CA, July 2225, 1996.
- **Program Committee member:** ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 2223, 1996.

Panels

- **Panelist:** CyberTech Global Conference: The Post-COVID Cyber Challenges in the Health Sector, UAE-Dubai (April 6, 2021).
- **Panel Organizer and Moderator:** USENIX Security Conference: The 2020 Election: Remote Voting, Disinformation, and Audit (August 12, 2020).
- **Panelist:** Cardozo Society Associated panel: Cybersecurity and Privacy Law in the Digital Era, Baltimore, MD (February 19, 2020).
- **Panelist:** Washington Post panel: Hacking Health, Washington DC (June 14, 2016).
- **Panelist:** Financial Cryptography Conference, Security & Privacy, Barbados (February 24, 2016).
- **Panelist:** RSA Conference, Social Networks Security Panel, San Francisco, CA (April 21, 2015).
- **Panelist:** Expert Witness in Mock Trial: FTC Data Security, 63rd American Bar Association Section of Antitrust Law Spring Meeting Washington DC, (April 15, 2015).
- **Panelist:** Security in Electronic Medical Records Databases, Medicine 2.0 Workshop, Haifa, Israel, (April 7, 2011).
- **Panelist:** Security in the Cloud, Workshop on Cloud Security, Israeli Defense Ministry, Tel Aviv, Israel, (February 15, 2011).

- **Panelist:** Securing Information Technology in Healthcare (SITH), Security and Usability of Electronic Health Records, Dartmouth College, NH, (May 17, 2010).
- **Panelist:** First Security and Privacy in Medical and HomeCare Systems Workshop (SPIMACS), Authentication in iHealthcare, Chicago, IL, (November 13, 2009).
- **Panelist:** Computers, Freedom, and Privacy Conference, Internet Voting for Overseas Americans, Washington DC, (June 4, 2009).
- **Panelist:** Workshop on Electronic Voting, Electronic Voting: Future Aspirations, Tel Aviv, Israel (May 18, 2009).
- **Panelist:** RSA Conference, Exploiting Online Games, San Francisco, CA (April 23, 2009).
- **Panelist:** American Association for the Advancement of Science, Revisiting the U.S. Voting System: A Research Inventory, Technology, Usability, and Security panel, Washington DC, (November 27, 2006).
- **Panelist:** California Secretary of State's Voting System Testing Summit, Security Panel, Sacramento, CA, (November 2829, 2005).
- **Panelist:** NIST Symposium on Voting System Threats, Configuration and Usability Threats, Gaithersburg, MD, (October 7, 2005).
- **Panelist:** Conference of State Supreme Court Chief Justices, Voting Technologies, Charleston, SC (August 1, 2005).
- **Panelist:** Workshop on observation of automated elections, The Carter Center, Atlanta, GA (March 18, 2005).
- **Panelist:** The Carter Center Venezuela Virtual Panel, (November, 2004).
- **Panelist:** Workshop on Voting, Vote Capture and Vote Counting, Harvard Kennedy School of Government, The Technologies of Voting, Cambridge, MA (June 1, 2004).
- **Panelist:** Computer Science and Telecommunications Board of The National Academy of Science Workshop on Dependable Software Systems, Case Study: Electronic Voting Washington D.C. (April 20, 2004).
- **Panelist:** USENIX Security 2003, Electronic Voting, Washington D.C. (August 6, 2003).
- **Panelist:** Democracy Now, 2003, Voter-Verifiable Elections: How Do We Get There?, Washington D.C. (November 23, 2003).
- **Panelist:** USENIX Security 2003, Electronic Voting, Washington D.C. (August 6, 2003).
- **Panelist:** IEEE Infocom 2002, Securing Wireless and Mobile Networks, Is It Possible?, New York City (June 25, 2002).
- **Participant:** 2002 Security Visionary Roundtable: A Roadmap for a Safer Wireless World, Washington D.C., (May 5-7, 2002).
- **Panelist:** Computers Freedom and Privacy 2002, Who Goes There? Privacy in Identity and Location Services, San Francisco (April 18, 2002).
- **Panel moderator:** Conference on Democracy and the Internet in an Enlarging Europe Overview of On-Line Voting: Systems and Issues, New York, NY (March, 2001).
- **Panelist:** Financial Cryptography 2001, The Business of Electronic Voting, Grand Cayman (February, 2001).
- **Panelist:** National Science Foundation E-voting workshop, Washington, D.C., (October, 2000).
- **Panelist:** 5th ACM Conference on Computer and Communications Security, Anonymity on the Internet, San Francisco, CA, (November, 1998).
- **Panelist:** Open Systems Security and ISSA Annual Conference, Securing the Web, Orlando, FL (March, 1998).

- **Panel organizer and moderator:** Implementation Issues for Electronic Commerce: What Every Developer Should Know. ISOC Symposium on Network and Distributed System Security, (March, 1998).
- **Panel organizer and moderator:** Downloadable Executable Content Past, Present and Future. ISOC Symposium on Network and Distributed System Security (February, 1997).
- **Panelist:** DIMACS Workshop on Network Threats, Web/Java Security Issues, New Brunswick, NJ (December 5, 1996).

Testimony

Before Government Bodies

- United States House Committee on Administration, Full Committee Hearing, Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House, Live via WebEx, (July 17, 2020).
- Maryland House, Expert Testimony, Hearing on HB 888, Consumer Protection, Security Features for Connected Devices, Economic Matters Committee, Annapolis, MD, (February 26, 2020).
- Maryland Senate, Expert Testimony, Hearing on SB 443 Security Features for Connected Devices, Finance Committee, Annapolis, MD, (February 19, 2020).
- Maryland Senate, Expert Testimony, Hearing on SB 553/HB 1276 Security Features for Connected Devices, Finance Committee, Annapolis, MD, (February 26, 2019). United States Pentagon, High Level Security Briefing on the Security of Embedded Devices (January 15, 2014).
- United States House Committee on Science, Space, and Technology, Full Committee Hearing Is My Data on Healthcare.gov Secure?, Washington, D.C., (November 19, 2013).
- United States House Committee on Oversight and Government Reform, hearing on electronic voting, Washington, D.C., (April 18, 2007).
- United States House Committee on Appropriations, hearing on ensuring the integrity of elections, Washington, D.C., (March 7, 2007).
- Maryland Senate Committee on Education, Health, and Environmental Affairs, Expert Testimony, Hearing on Senate Bill 392 for VoterVerified Records in Voting Systems, Annapolis, MD, (February 22, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, Hearing on House Bill 18 for improving voting systems in Maryland, Annapolis, MD, (February 1, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, Hearing on House Bill 244 requiring a voter verified paper record for voting machines in Maryland, Annapolis, MD, (February 1, 2006).
- United States Election Assistance Commission, Hearing on Voluntary Voting Systems Guidelines, Expert Testimony, Panel on Voter Verified Paper Audit Trail, Washington D.C. (June 30, 2005).
- Senate hearing: Voting in 2004: A Report to the Nation on America's Election Process, Expert Testimony, Absentee Ballot Panel, Dirksen Senate Office Building, Washington, DC (December 7, 2004).
- United States Election Assistance Commission, Technical Guidelines Development Committee, Technology Panel, Expert Testimony, Public Hearings on Computer

Security and Transparency, National Institute of Standards and Technology, Gaithersburg, MD, (September 20, 2004).

- United States House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Expert Testimony, Hearing on Electronic Voting, Washington, D.C. (July 20, 2004).
- United States House Committee on House Administration, Expert Testimony, Hearing on Security of Electronic Voting, Washington, D.C. (July 7, 2004).
- United States Federal Trade Commission, Written Expert Testimony, on a proposed Do Not Email Repository, (May 10, 2004).
- United States Election Assistance Commission, Expert Testimony, Hearing on Electronic Voting Security, Technology Panel, Washington D.C. (May 5, 2004).

As an Expert in Litigation

- Robocast vs. **Netflix Inc**, Case # 1:22-cv-00305-JLH-CJB, Latham & Watkins, United States District Court, District of Delaware. (patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Washington DC, (August 28, 2024).
- Epic Games, Inc & Anor vs. **Apple Inc & Anor.**, Case # NSD 1236 of 2020, Gibson Dunn, Federal Court of Australia, District of New South Wales. (App Store Security & Privacy)
 - Expert Testimony at Trial, Melbourne, Australia (May 29, 2024).
- **Proxense, LLC**, vs. Google., Case # 6:23-cv-00320-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent claim construction)
 - Expert Testimony at deposition, Key West, FL (December 18, 2023).
- **Softex LLC** vs Absolute Software Corporation, Dell Technologies Inc, and HP Inc, Case # 1:22-cv-01309-DAE; McKool Smith, United States District Court, Western District of Texas. (Patent Claim Construction)
 - Expert Testimony at deposition, Key West, FL (November 27, 2023).
- **Milliman, Inc** and Vigilytics LLC, vs. Gradient A.I. Corp., Case # 1:21-cv-10865-NMG; K&L Gates, United States District Court, District of Massachusetts. (Patent Claim Construction, Patent Infringement, Patent Validity, Trade Secret)
 - Expert Testimony at deposition, Annapolis, MD (November 27, 2023).
 - Expert Testimony at deposition, Annapolis, MD (November 17, 2022).
- Microsoft Corporation vs. **Mediapointe, Inc**, Case # 2:22-cv-01009-MCS-MRW; Susman Godfrey, United States District Court, Central District of California. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (September 29, 2023).
- Akamai Technologies, Inc vs. **Mediapointe, Inc**, Case # 2:22-cv-06233-MCS-AFM; Susman Godfrey, United States District Court, Central District of California. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (September 22, 2023).
- Lauri Valjakka vs. **Netflix Inc**, Case # 4:22-cv-01490-JST, Perkins Coie, United States District Court, Northern District of California. (patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Annapolis, MD (September 8, 2023).
- **TecSec Inc** vs. Oracle, Case # 1:10CV 115 LO-TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement, Patent Validity)

- Expert Testimony at deposition, Annapolis, MD (June 13, 2023).
- Expert Testimony at deposition, Annapolis, MD (September 11, 2020).
- Global Eticket Exchange Ltd. vs. **TicketMaster LLC**, Case # 6:21-cv-00399-ADA, Fish & Richardson, United States District Court, Western District of Texas. (Patent Non-infringement and validity)
 - Expert Testimony at Trial, Waco, TX (May 3, 2023).
 - Expert Testimony at Deposition, Annapolis, MD (January 31, 2023).
 - Expert Testimony at Deposition, Annapolis, MD (January 16, 2023).
- **Fanduel, Inc** vs. Winview, Inc, IPR 2022-01306, ArentFox Schiff, US Patent Trial and Appeal Board. (Patent Invalidity)
 - Expert Testimony at deposition, Annapolis, MD (April 20, 2023).
- **Fanduel, Inc** vs. Winview, Inc, IPR 2022-01307, ArentFox Schiff, US Patent Trial and Appeal Board. (Patent Invalidity)
 - Expert Testimony at deposition, Annapolis, MD (April 19, 2023).
- **TecSec Inc** vs. Cisco, Case # 1:10-CV 115 LO-TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement, Patent Validity)
 - Expert Testimony at deposition, Washington DC (April 12, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 14, 2020).
- **WSOU Investments, LLC**, vs. Cisco Systems Inc., Case # 6:21-cv-00128-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (March 30, 2023).
 - Expert Testimony at deposition, Annapolis, MD (January 18 & 19, 2023).
- Finjan vs. **Palo Alto Networks**, Case # 4:14-CV-04908-PJH, Morrison and Foerster, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Annapolis, MD (March 17, 2022). (*Patent Non-infringement and invalidity*)
 - Expert Testimony at Deposition, Annapolis, MD (March 15, 2022). (*Patent Non-infringement and invalidity*)
 - Expert Testimony at Deposition, Pikesville, MD (August 16, 2021). (*Claim Construction*)
- Centripetal Networks, Inc. vs. **Keysight Technologies, Inc.**, Investigation No. 337-TA-1314-MJM, Reed Smith LLP, United States International Trade Commission (ITC). (Patent Non-infringement & Domestic Industry Technical Prong)
 - Expert Testimony at Trial, Washington DC (March 6, 2023).
 - Expert Testimony at Deposition, Las Vegas, NV (December 2, 2022).
- **Proxense, LLC**, vs. Samsung Electronics Co., Case # 6:21-cv-00210ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (January 12, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 30, 2022).
 - Expert Testimony at deposition, Annapolis, MD (September 29, 2022).
- **US Dominion, Inc.** vs. Fox News Network, Case # N21C-03-257-EMD, Susman Godfrey, United States District Court, District of Delaware. (Defamation)
 - Expert Testimony at deposition, Annapolis, MD (January 10, 2022).

- **Rimini Street, Inc.** vs. Oracle International Corporation, et. al., Case # 2:14-CV-01699 LRHCWH, Gibson Dunn, United States District Court, District of Nevada. (Software security)
 - Expert Testimony at trial, Las Vegas, NV (December 9, 2022).
 - Expert Testimony at deposition, Baltimore, MD (August 30, 2018).
- **IOEngine, LLC**, vs. Ingenico Inc., Case # 1:18-cv-826 WCB; Dechert LLP, United States District Court, District of Delaware. (Patent Infringement & Patent Validity)
 - Expert Testimony at trial, Wilmington, DE (July 12 & 14, 2022).
 - Expert Testimony at deposition, Annapolis, MD (January 28, 2022).
 - Expert Testimony at deposition, Bonita Springs, FL (January 19, 2022).
- **WSOU Investments, LLC**, vs. Microsoft Corporation, Case # 6:20-cv-00464-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement and Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (May 15 & 16, 2022).
- **10Tales Inc.** vs. TikTok PTE. LTD., Case # 4:21-cv-3868-YGR; Cozen O'Connor, United States District Court, Northern District of California. (Patent Claim Construction)
 - Expert Testimony at deposition, Annapolis, MD (May 11, 2022).
- **IOEngine, LLC**, vs. PayPal Holdings, Inc., Case # 1:18-cv-452-WCB; Dechert LLP, United States District Court, District of Delaware. (Patent infringement)
 - Expert Testimony at deposition, Bonita Springs, FL (January 18, 2022).
 - Expert Testimony at deposition, Bonita Springs, FL (January 26, 2022).
- AGIS Software Development LLC vs. **Uber Technologies Inc.**, Case # 2:21-cv-00026-JRG-RSP, Gibson Dunn, United States District Court, Eastern District of Texas. (Non-infringement)
 - Expert Testimony at Deposition, Annapolis, MD (December 22, 2021).
- Sable Networks vs. **Splunk Inc.**, Case # 5:21-CV-00040-RWS, Morrison and Foerster, United States District Court, Eastern District of Texas. (Claim Construction)
 - Expert Testimony at Deposition, Annapolis, MD (December 13, 2021).
- Huawei Technologies Co. vs. **Verizon Communications Inc.**, Case # 6:20-CV-00090, Quinn Emanuel, United States District Court, Western District of Texas. (Patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Pikesville, MD (July 1, 2021).
- Epic Games, Inc. vs. **Apple Inc.**, Case # 4:20-cv-05640-YGR-TSH, Gibson Dunn, United States District Court, Northern District of California. (Sherman Act)
 - Expert Testimony at Trial, Oakland, CA (May 20-21, 2021).
 - Expert Testimony at Deposition, Pikesville, MD (March 26, 2021).
- Philips North America LLC ; Koninklijke Philips N.V. vs. **Summit Imaging Inc.**, Case # 2:19cv01745JLR, Seed IP, United States District Court, Western District of Washington at Seattle. (DMCA and Copyright)
 - Expert Testimony at deposition, Pikesville, MD (March 16, 2021).
- **California Physicians Service, Inc D/B/A Blue Shield of California** vs. Healthplan Services Inc, Case # 3:18-cv-3730 Latham & Watkins, United States District Court, Northern District of California. (Contract Dispute: Software Quality and Security)
 - Expert Testimony at Deposition, Pikesville, MD (March 9, 2021).

- Finjan vs. **Qualys Inc.**, Case # 4:18-cv-07229-YGR, Wilson Sonsini, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at Deposition, Pikesville, MD (March 4, 2021).
- Finjan vs. **Sonicwall Inc.**, Case # 5:17-cv-04467-BLF-HRL, Duane Morris, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at deposition, Pikesville, MD (October 30, 2020).
 - Expert Testimony at deposition, Pikesville, MD (October 29, 2020).
- **Blackberry Limited** vs. Facebook, Inc, Case #2:18-cv-01844 (KSx), Quinn Emanuel Urquhart & Sullivan, LLP, United States District Court, Central District of California. Expert Testimony at Deposition, Baltimore, MD (December 20, 2019). (patent infringement & patent validity)
- **Netfuel, Inc.** vs. Cisco Systems, Inc, Case # 5:18-cv-2352-EJD, Susman Godfrey, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Baltimore, MD (December 16 & 17, 2019). (patent infringement & patent validity)
 - Expert Testimony at Deposition, Baltimore, MD (June 11, 2019). (patent infringement)
 - Expert Testimony at Markman Hearing, San Jose, CA (February 28, 2019). (courtroom tutorial)
 - Expert Testimony at deposition, Baltimore, MD (December 20, 2018). (claim construction)
- **Symantec Corporation** vs. Zscaler, Inc., Case # 3:17-CV-04414-JST, Baker Botts, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Baltimore, MD (December 6, 2019). (patent infringement)
 - Expert Testimony at Deposition, Baltimore, MD (August 2, 2019). (Assignor Estoppel)
- Koninklijke Philips vs. **Microsoft Inc**, Case # 4:18-cv-01885-HSG, Perkins Coie, United States District Court, Northern District of California. (patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Baltimore, MD (July 17, 2019).
- **Cypress Lake Software**, Inc. vs. Samsung Electronics & Dell Inc, Case # 6:18-cv-030-JKD and 6:18cv0138JDK, Garteiser Honea, United States District Court, Eastern District of Texas. (patent infringement and patent validity)
 - Expert Testimony at Deposition, Baltimore, MD (July 10/11, 2019).
- Finjan vs. **Juniper Networks**, Case # 3:17-cv-05659-WHA , Irell and Manella, United States District Court, Northern District of California.
 - Expert Testimony at deposition, Baltimore, MD (April 2, 2019). (patent Non-infringement)
 - Expert Testimony at deposition, San Francisco, CA (March 9, 2019). (patent Non-infringement)
 - Expert Testimony at trial, San Francisco, CA (December 13, 2018). (patent Non-infringement and invalidity)

- Expert Testimony at deposition, Baltimore, MD (November 9, 2018). (patent Non-infringement and invalidity)
- Expert Testimony at deposition, Baltimore, MD (July 6, 2018). (patent Non-infringement)
- Expert Testimony at deposition, Baltimore, MD (June 12, 2018). (patent Non-infringement)
- Grace et. al. vs. **Apple Inc.**, Case # 5:17-CV-00551LHK (NC), Durie Tangri, United States District Court, Northern District of California. (class action)
 - Expert Testimony at deposition, Towson, MD (September 26, 2018).
- Grace et. al. vs. **Apple Inc.**, Case # 5:17-CV-00551-LHK (NC), Kirkland & Ellis, United States District Court, Northern District of California. (class certification)
 - Expert Testimony at deposition, Pikesville, MD (July 3, 2018).
- **F5 Networks, Inc.** vs. Radware, LTD., IPR 2017-00124, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (January 24, 2018).
- **Amazon.com Inc., Hulu, LLC, and Netflix, Inc.** vs. Uniloc Luxembourg S.A., IPR 201700948, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (October 9, 2017).
- Phishme, Inc. vs. **Wombat Technologies, Inc.**, Case # 16403-LPS-CJB, K&L Gates, United States District Court, Delaware. (patent claim construction)
 - Expert Testimony at deposition, Washington DC, (October 5, 2017).
- Finjan vs. **Symantec Corporation.**, Case # 14-cv-02998-HSG, Quinn Emanuel, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at deposition, Baltimore, MD (September 14-15, 2017).
- **Kudelski SA, Nagra USA, Inc., Nagravision SA, and OpenTV, Inc.** vs. Comcast Corporation, Case # 2:16-cv-1362-JRG, Covington, United States District Court, Eastern District of Texas. (patent claim construction).
 - Expert Testimony at deposition, Baltimore, MD (September 1, 2017).
- **F5 Networks, Inc.** vs. Radware, LTD., IPR 2017-00124, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 10, 2017).
- Intellectual Ventures vs. **JP Morgan Chase & Co.**, Case # 1:13-cv-03777, Kirkland & Ellis, United States District Court, Southern District of New York. (Patent Non-infringement).
 - Expert Testimony at deposition, Baltimore, MD (June 1, 2017).
- Nader AsghariKamrani and Kamran AsghariKamrani vs. **United Services Automobile Association.** Case # 2:15-CV-478, Fish & Richardson, United States District Court, Eastern District of Virginia. (Patent Written Description Support related to Inequitable Conduct).
 - Expert Testimony at trial, Norfolk, VA (April 21, 2017).
 - Expert Testimony at deposition, Baltimore, MD (March 21, 2017).
- **Sabre GLBL Inc.** vs. HP Enterprise Services LLC. Case # 1310022761, JAMS Binding Arbitration Hearing, Dallas, TX (Contract dispute).
 - Expert Testimony at arbitration hearing, Dallas, TX (April 5, 2017).

- **Al Cioffi et. al.** vs. Google, Case # 2:13cv103JRGRSP, Vasquez, Benisek & Lindgren, United States District Court, Eastern District of Texas. (patent Infringement).
 - Expert Testimony at trial, Marshall, TX (February 7, 2016).
 - Expert Testimony at deposition, Baltimore, MD (September 26, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01979, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (November 14, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2016-00151, Morrison & Foerster, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 19, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01974, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 2, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-02001 & IPR 2016-00157, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 26 & 27, 2016).
- **Amazon.com, Inc** vs. Zitovault, LLC, IPR 2016-00021, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 22, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01979, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (May 20, 2016).
- Vir2us Inc. v. **Invincea, Inc. and Invincea Labs, LLC**, Case # 2:15-cv-l62; Cooley, United States District Court, Eastern District of Virginia. (Patent Non-infringement and Invalidity)
 - Expert Testimony at deposition, Reston, VA (April 20, 2016).
- TVIIM. v. **McAfee Inc.**, Case # 3:13-cv-04545-VC; Wilmer Hale, United States District Court, District of N. California. (Patent Non-infringement and Invalidity)
 - Expert Testimony at trial, San Francisco, CA (July, 2015).
 - Expert Testimony at deposition, Baltimore, MD (February, 2015).
- Intellectual Ventures vs. **Symantec**, Case # 1:10-cv-01067-LPS; Latham & Watkins, United States District Court, District of Delaware. (Patent Invalidity)
 - Expert Testimony at trial, Wilmington, DE (February, 2015).
 - Expert Testimony at deposition, Baltimore, MD (May, 2013).
- **Rovi Solutions & Veracode** vs. Appthority, Case # 1210487-DPW; Goodwin Procter, United States District Court, District of Massachusetts. (Patent Infringement and Validity)
 - Expert Testimony at trial, Boston, MA (August 11, 2014).
 - Expert Testimony at deposition, Baltimore, MD (April 4, 2014).
- **Juniper** vs. Palo Alto Networks, Case # 1:11-CV-01258-SLR; Irell & Manella, United States District Court, District of Delaware. (Patent Infringement)
 - Expert Testimony at trial, Wilmington, DE (February, 2014).
 - Expert Testimony in court hearing, Wilmington, DE (November 14, 2013).
 - Expert Testimony at deposition, Baltimore, MD (June, 2013).
- Prism Technologies. v. **Adobe Systems Inc.**, Case # 8:10-cv-00220-LEST-DT; DLA Piper, United States District Court, District of Nebraska. (Patent Invalidity)

- Expert Testimony at deposition, Baltimore, MD (August, 2012).
- Finjan Inc. vs. **McAfee, Inc.**, Case # 10593 (GSM), Kirkland & Ellis, United States District Court, District of Delaware. (Patent Non-infringement)
 - Expert Testimony at deposition, Washington, DC (June, 2012).
- Avaya Inc. vs. **Telecom Labs Inc., TeamTLI.com Corp., and Continuant Technologies**, Case # 3:06-cv-02490 (GEB); K&L Gates, United States District Court, District of New Jersey. (Contract Dispute)
 - Expert Testimony at deposition, Newark, NJ (August, 2011).
- **Lear Automotive** vs. Johnson Controls Inc (JCI), Case # 04-CV-73461; Flachsbarth & Greenspoon, United States District Court, Eastern District of Michigan. (Patent Infringement and Validity)
 - Expert Testimony at trial, Detroit, MI (February, 2011).
 - Expert Testimony at deposition, Baltimore, MD (December, 2005).
- **TecSec Inc** vs. International Business Machines Corporation, Case # 1:10-CV-115-LMB/TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement)
 - Expert Testimony at deposition, Newark, NJ (November, 2010).
- **Echostar Satellite Corporation** vs. NDS Group, Case # SA-CV-03950-DOC(JTL); T. Wade Welch & Associates, United States District Court, Central District of California. (Copyright and DMCA)
 - Expert Testimony at trial, Santa Ana, CA (April, 2008).
 - Expert Testimony at deposition, Santa Ana, CA (April, 2008).
 - Expert Testimony at deposition, Baltimore, MD (October, 2007).
- **Web.com Inc** vs. The Go Daddy Group Inc., Case # CV-0701552-PHX-MHM; Graves Law Office, United States District Court, Arizona. (Patent Infringement)
 - Expert Testimony at Markman hearing, Phoenix, Az (July, 2008).
 - Expert Testimony at deposition, Baltimore, MD (May, 2008).
- z4 Technologies vs. **Microsoft & Autodesk**, Case # 2:04-CV-00335-LED; Fish & Richardson, United States District Court, Eastern District of Texas. (Patent Non-Infringement and Invalidity)
 - Expert Testimony at trial, Tyler, TX, (April, 2006).
 - Expert Testimony at deposition, Washington DC (January, 2006).
- **Linda Schade** vs. Linda Lamone et. al., Trial on the Legality of Paperless Voting Machines in Maryland. (Adequacy of Voting Equipment)
 - Expert Testimony at trial, Annapolis, MD (August 25, 2004).

Awards

- 2020, **Best Paper Award**, in the category of Mobile & Wireless Computing, 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), October, 2020.
- 2020, **Best Paper Award**, in the category of Image Processing & Multimedia Technology, 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), October, 2020.
- IEEE Computer Society Technical Committee on Security and Privacy, **Distinguished Service Award**, May, 2020.
- **Fulbright Scholar** in Israel at Tel Aviv University, academic year 2010-2011.

- 2009, **Google Research Award**, Securing Medical Records on Smartphones.
- Chosen as one of **54 favorite people, places and things in Jewish Baltimore**, Baltimore Jewish Times, February 22, 2008.
- 2007 **Award for Outstanding Research in Privacy Enhancing Technologies**, for Security Analysis of a Cryptographically Enabled RFID Device (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
- 2005 **Best Student Paper Award** at the 14th USENIX Security Symposium, Security Analysis of a Cryptographically Enabled RFID Device (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
- 2004 Electronic Frontiers Foundation **Pioneer Award**.
- **Baltimorean of the Year**, Baltimore Magazine, January, 2004.
- 2001 Index on Censorship **Freedom of Expression Award** for the Best Circumvention of Censorship for the Publius project.
- 2000 **Best Paper Award** at the 9th USENIX Security Symposium, A robust, tamper-evident and censorship-resistant web publishing system (with Marc Waldman and Lorrie Cranor).
- 1999 **Best Paper Award & Best Student Paper Award** at the 8th USENIX Security Symposium, The Design and Analysis of Graphical Passwords (with Ian Jermyn, Alain Mayer, Fabian Monroe, and Michael K. Reiter).
- 1996 Coauthor of **Best Student Paper**, Building Systems that Flexibly Control Downloaded Executable Content, at the 6th USENIX UNIX Security Symposium. Student: Trent Jaeger.
- 1992 National Science Foundation **Fellowship Summer Institute in Japan**
- 1986 **Branstrom Prize**, University of Michigan

Technical Advisory Boards

Current Positions

Qualytics: Data Quality Assurance
RunSafe: Binary rewriting to protect software
Flohom: Floating homes

Past Technical Advisory Board Positions with Successful Exits

Arbor Networks: Acquired by Danaher, August, 2010.
Authentica: Acquired by EMC Corporation, March, 2006.
Fortify Software: Acquired by Hewlett Packard, September 2010.
Gilian Technologies: Acquired by Breach Security, Inc, July, 2004.
Hx Technologies: Acquired by MEDecision, May, 2009.
Indigo Security: Acquired by Tablus, February, 2005.
NeoPath Networks: Acquired by Cisco, April, 2007.
Netscaler: Acquired Citrix Systems, August, 2005.
SiteAdvisor: Acquired by McAfee, April, 2006.
Tablus: Acquired by EMC Corporation, August, 2007.
ZeroFox: Public Offering via SPAC, July, 2022.

APPENDIX B

APPENDIX B

Citation	Source Language	Notes
Ex. 1003, ¶58	Generally speaking, Landi relates to systems and methods for protecting patient privacy when health care information is shared between various healthcare entities to maintain compliance with HIPAA regulations by using a token generation and matching system to de-identify patient data. Ex. 1008, 1:14-16; 2:30-34; 3:52-57. Landi does this by generating an encrypted ID for individuals which represents one or more items of individual identifying information. <i>Id.</i> , 2:46-49.	This portion of Dr. Clark's declaration does not discuss token matching or querying the central server.
Ex. 1008, 1:14-16.	The present invention relates, in general, to systems and methods for protecting patient privacy when healthcare information is shared between various healthcare entities and, in	This portion of Landi describes the general invention. It does not mention token matching or querying the central server.
Ex. 1008, 2:30-34.	Exemplary embodiments of the invention generally include systems and methods for	This portion of Landi describes the general invention. It does not mention

	protecting individual privacy (e.g., patient privacy) when private information (e.g., health care information) is shared between various entities (e.g., healthcare entities). More specifically, exemplary	token matching or querying the central server.
Ex. 1008, 3:52-57.	encryption method. Advantageously, as explained below, systems and methods according to the invention for de-identifying/re-identifying patient data can be implemented for various purposes such as research, public health or healthcare operations, while maintaining compliance with regulations based on HIPAA for protecting patient privacy.	This portion of Landi discusses the advantageous of the invention; but it does not get into token matching or querying the central server.
Ex. 1003, ¶202	Landi sets forth in detail a de-identification method that a POSA would understand can be implemented in Dick. Landi describes a token matching system used to de-identify patient records to comply with HIPAA. More specifically, Landi describes how healthcare	This portion of Dr. Clark's declaration cites to Landi at 4:19-29, which is reproduced below. As can be seen, clearly this portion of Landi does not mention token matching or querying the central server.

	providers or sources can de-identify their records by creating an encrypted token, then release the de-identified records to a central data server where they can be processed, e.g., queried for research and healthcare monitoring. Ex. 1008, 4:19-29.	
Ex. 1008, 4:19-29.	The patient data processing systems (20-1-20-n) are operated at different clinical sites by different healthcare organizations (including, but not limited to, doctors, health care providers, institutions, associations, organizations, hospitals, etc.). In the exemplary embodiment, each clinical site releases de-identified patient data records to a third-party entity that operates the central patient data processing system (30), wherein the collected de-identified data records can be processed for purposes of e.g., research, health care monitoring, etc. In addition, the central	This portion of Landi discusses processing de-identified patient records, but does not mention <i>token matching</i> specifically, or querying the central server, generally.

	surveillance system (50) may be operated and controlled by a governmental agency	
Ex. 1003, ¶218	Landi also describes how this token matching system would work for querying for patient records associated with a clinical trial where “each time data is collected, the patient should be de-identified in the same way” in order to create a first token to be used to query the patient records. <i>Id.</i>, 9:43-60. Landi also other examples of querying the de-identified patient data. <i>Id.</i> 7:3-10; 8:47-55; 10:52-63; 11:23-29; claim 15 (“using the encrypted ID . . . to recognize a subject patient of patient data records collected at different times.”). Therefore, a POSA implementing Landi’s token matching system into Dick would understand that each token produced for the query on the Requester’s Server matches a corresponding token in Medical Information Repository’s de-identified patient records. In that way the relevant	Each of the section of Landi that Dr. Clark cites to are discussed below. None describe token matching or querying the central server. Dr. Clark’s statements in this paragraph are purely conclusory and rely on faulty logic. By concluding without evidence that Landi teaches token matching and querying the central server, he assumes what he should have set out to prove.

	de-identified healthcare information related to patients in a clinical trial can be retrieved in compliance with HIPAA.	
Ex. 1008, 9:43-60	Moreover, systems and methods according to the present invention for de-identifying patient data can be implemented for clinical trials and research studies, which is common in the medical industry. The following requirements are common for experiments and clinical trials: (1) to comply with HIPAA, analysis must be done on de-identified data when the persons analyzing patient data are not associated with the provider organization; (2) data is collected at various points of time and analyses are performed after each data collection; (3) each time data is collected, the patient should be de identified in the same way (e.g., it is critical to know that "de-identified patient 24 from a first round of collection is also present in a second round and is	Element (3) in this paragraph by Landi is the pertinent language, where the same Encrypted IDs are used for the same patients for consistent de-identification at the point in time when data is collected from the patent data processing systems. This paragraph and similar text throughout Landi, including Claim 15, do not teach token matching. Instead, they teach using the same encryption technique for consistent de-identification of the same patient.

	still de-identified as "de-identified patient 24); and (4) the hospital (or other provider of de-identified patient information) may or may not want the ability to re-identify the data. Such uses would probably come under the limited data set provisions of HIPAA rather than fully de-identified data.	
Ex. 1008, 7:3-10	The central patient data processing system (30) comprises a repository of persistently stored de-identified patient data records (35) containing de-identified (encrypted) patient identifying information, which are collected from the different clinical sites. The central patient data processing system (30) comprises one or more data processing engines (37) that are used for processing the de-identified patient data (35) for one or more given applications. The central patient data pro	This paragraph merely discusses what data is being stored at the central server. It does not teach or suggest token matching or how the central server receives or responds to queries for patent data.

Ex. 1008, 8:47-55	The public keys are freely distributable (no HIPAA issues) to healthcare organizations for de-identification of patient data. Moreover, the public keys can be used to produce a unique, reproducible encrypted version of patient identifying information. Since the encryption is reproducible, the same patient can be recognized at different times (i.e., consistent de-identification can be achieved over episodic collection events) even though the identity of the person remains unknown.	The public keys are freely distributable <i>to healthcare organizations</i> for <i>de-identification of patient data</i>. Note that this paragraph concerning the keys being freely available is truncated in the petition and expert report. The full statement clarifies that the public keys are used for de-identification <i>of patient data</i>. The healthcare organization that performs this function has to have patient data to perform de-identification.
Ex. 1008, 10:52-63	Next, the identified patient data records to be de-identified and disclosed are accessed from a database owned and operated by the disclosing entity (step 51), and the identified patient data records and encryption key are input to an encryption system (step 52) to generate de-identified patient data records. In accordance with	This step shows how patient records are de-identified. No querying the central server here.

	HIPAA regulations, all de-identification of patient data records must occur at the clinical site of the disclosing party. For example, as a general rule, a third-party is not permitted to remove identified patient data records from a hospital and then de-identify the identified patient data records at a later time, but there may be exceptions to this rule. The encryption system for de-identifying the	
Ex. 1008, 11:23-29	It is to be appreciated that since each Encrypted ID is a unique reproducible encrypted version of patient identifying information, the process preserves patient uniqueness to enable to the same patient to be recognized at different collection times. In other words, this process ensures that if data is collected more than once from a particular patient, the patient will be mapped to the same Encrypted ID.	Again, the same Encrypted IDs are used for the same patients for consistent de-identification at the point in time when data is collected from the patent data processing systems. This paragraph and similar text throughout Landi, including Claim 15, do not teach token matching. Instead, they teach using the same encryption technique

		for consistent de-identification of the same patient.
Ex. 1008, claim 15	The method of claim 12, further comprising using the encrypted ID . . . to recognize a subject patient of patient data records collected at different times.	Claim 12 depends from claim 1, which is a method that is performed by the patient data processing not the central data server. From specification to show this is not token matching: “Since the encryption is reproducible, the same patient can be recognized at different times (i.e., consistent de-identification can be achieved over episodic collection events) even though the identity of the person remains unknown.” 8:51–55.
Ex. 1008, 4:40-47	(“the public keys . . . are used for de-identifying (encrypting) one or more items of patient identifying information (i.e., information that	This paragraph merely discusses what public keys are for, not token matching or how the central server is queried.

	could be used for identifying the patient) to generate an encrypted version of the patient identifying information (referred to herein as ‘Encrypted IDs)’.”).	
Ex. 1008, 9:52-56	(“each time data is collected, the patient should be de-identified in the same way (e.g., it is critical to know that de-identified patient 24 from a first round of collection is also present in a second round and is still de-identified as de-identified patient 24).”).	Again here, the same Encrypted IDs are used for the same patients for consistent de-identification at the point in time when data is collected from the patent data processing systems. This paragraph and similar text throughout Landi, including Claim 15, do not teach token matching. Instead, they teach using the same encryption technique for consistent de-identification of the same patient.
The de-identified medical records are stored in a central	4:11-28: FIG. 1 illustrates a high-level schematic diagram of a system (10) according to one exemplary embodiment of the invention wherein	Already discussed above. This is a system overview of FIG. 1; it does not get into any specifics for how the

data server that can be queried, much like Dick's medical repository. Ex. 1008, 4:11-28, 7:3-38, 8:16-19, 8:61-63, 10:15-54, 11:52-63 ("can readily be searched").	a secured encryption scheme is implemented for protecting patient privacy when patient data is shared between different entities. In general, the exemplary system (10) comprises a plurality of patient data processing systems (20-1-20-n), a central patient data processing system (30), a trusted broker system (40), and a central surveillance system (50). The patient data processing systems (20-1-20-n) are operated at different clinical sites by different healthcare organizations (including, but not limited to, doctors, healthcare providers, institutions, associations, organizations, hospitals, etc.). In the exemplary embodiment, each clinical cite releases de-identified patient data records to a third-party entity that operates the central patient data processing system (30), wherein the collected de-identified data records can be processed for	central server works, nor does it discuss token matching or querying the central server.
---	---	---

	purposes of e.g., research, health care monitoring, etc.	
	7:3-38 – The central patient data processing system (30) comprises a repository of persistently stored de-identified patient data records (35) containing de-identified (encrypted) patient identifying information, which are collected from the different clinical sites. The central patient data processing system (30) comprises one or more data processing engines (37) that are used for processing the de-identified patient data (35) for one or more given applications.	Already discussed above.
	8:16-19 – Based on the teachings herein, one of ordinary skill in the art can readily envision various system architectures that may be implemented for sharing patient data, and such	Generic / boilerplate language but no specific discussion or callback to token matching or querying the central server.

	architectures will vary depending on the application.	
	8:61-63 – Systems and methods according to the invention for de-identifying patient data can be implemented for various purposes such as research, public health or healthcare operations.	Merely discusses de-identifying, not token matching or querying the central server.
	10:15-54 – FIG. 3 is a flow diagram illustrating a method for de-identifying patient data according to an exemplary embodiment of the invention. For example, FIG. 3 illustrates a method by which one or more clinical sites (e.g., hospitals, doctors, etc.) can de-identify patient data for purposes of disclosing/distributing the de-identified patient data to one or more third-party entities (e.g., governmental agency, research agency, or medical service provider, etc.) for a particular application, while ensuring patient	This is an introduction to Figure 3, which is about de-identifying at step 50, not querying repository.

	privacy. In one exemplary embodiment of the invention, FIG. 3 depicts an HIPAA compliant de-identification and disclosure process. In this regard, the disclosing and receiving parties can execute a "data use agreement" or "restricted access agreement", for example, which limits the distribution of the de-identified records, whereby the recipient agrees to restrictions on who can use or receive the data and for what purposes. Referring now to FIG. 3, a method for de-identifying patient data includes an initial step where a disclosing entity (e.g., hospital) will obtain encryption/decryption keys from a trusted entity (step 50), which are to be used for de-identifying and re-identifying patient data that is owned by the disclosing entity. In one embodiment of the invention using asymmetric key encryption, the encryption/decryption keys comprise a public/private key pair that is	
--	--	--

	associated with that disclosing entity. A public key cryptographic process for generating a public/private key pair can be implemented using an asymmetric encryption method such as RSA, DSA or PGP. In another embodiment using symmetric key encryption, a private key is generated for the disclosing entity, which is used for both encrypting and decrypting patient data. As noted above, in one exemplary embodiment of the invention, the encryption keys can be generated and securely disseminated by a trusted certificate authority (CA). In another embodiment, the third-party entity that collects the de-identified data may be authorized to provide a trusted service of generating and issuing the encryption keys. Next, the identified patient data records to be de-identified and disclosed are accessed from a	
--	---	--

	database owned and operated by the disclosing entity (step 51), and the identified	
	11:52-63 – “As noted above, structured patient data is typically maintained in database tables, wherein the patient data elements are known a priori and can readily be searched.”	This paragraph is referring to structured data records <i>at the patient data processing systems</i> for de-identification purposes. This is NOT talking about the central servers. This is a blatant misrepresentation of Landi.