

**UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD**

DATAVANT, INC.,

Petitioner,

CERTIFIED COPY

v.

VIGILYTICS LLC,

Patent Owner.

**Case 2024-00226 (US Patent No. 9,118,641)
Ref. 25412-0020IP1
Proceeding No. IPR2024-00226**

VIDEOCONFERENCE DEPOSITION OF

DR. PAUL CLARK

September 26, 2024

Page 1 - 101

9:38 a.m. - 2:08 p.m. EST

REPORTED BY:

Tamara L. Houston

CA CSR No. 7244, RPR, CCRR No. 140

Job Number 142600

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

**REMOTE VIDEOCONFERENCE DEPOSITION OF DR. PAUL
CLARK, taken on behalf of the Patent Owner, commencing
from 9:38 a.m. to 2:08 p.m. EST, Thursday, September 26,
2024, before Tamara L. Houston, CSR No. 7244, CCRR, RPR.**

APPEARANCE OF COUNSEL:

On behalf of the Petitioner:

**VENABLE LLP
BY: JUSTIN J. OLIVER, ESQ.
600 Massachusetts Avenue, NW
Washington, DC 20001
(202) 721-5423
joliver@venable.com**

On behalf of the Patent Owner and Witness:

**FISH & RICHARDSON, P.C.
BY: NICHOLAS STEPHENS, ESQ.
RISHA GUPTA, ESQ.
JEFFREY BARCLAYM, ESQ.
INDRANIL SARKER, ESQ.
3200 RBC Plaza
60 South Sixth Street
Minneapolis, Minnesota 55402
(612) 335-5070**

THE SULLIVAN GROUP OF COURT REPORTERS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

INDEX TO EXAMINATION

WITNESS: DR. PAUL CLARK

EXAMINATIONS	PAGE
Mr. Stephens.....	6

QUESTIONS INSTRUCTED NOT TO ANSWER

Page Line

NONE

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

INDEX TO EXHIBITS

DR. PAUL CLARK

DATAVANT, INC. vs. VIGILYTICS LLC

September 26, 2024

Tamara L. Houston, CSR No. 7244, CRR No. 140, RPR

EXHIBIT	DESCRIPTION	PAGE
----------------	--------------------	-------------

--o0o--

(Exhibits marked electronically.)

1 Thursday, September 26, 2024, 9:38 a.m.

2 --000--

3 Whereupon, DR. PAUL CLARK, having been
4 called as a witness was duly sworn
5 to tell the truth, the whole truth,
6 and nothing but the truth testified
7 as follows:

8 EXAMINATION BY MR. STEPHENS:

9 Q. Good morning, Dr. Clark.

10 A. Morning.

11 Q. My name is Nick Stephens. I'm an attorney
12 with Fish & Richardson. I'll be taking the deposition
13 today on behalf of the patent owner, Vigilytics LLC.

14 I'm joined by my colleagues Indranil Sarkar,
15 Rishi Gupta, and Jeffrey Barclay, each with Fish &
16 Richardson.

17 Would counsel for Petitioner like to make your
18 appearance?

19 MR. OLIVER: Justin Oliver of Venable on
20 behalf of the Petitioner, Datavant.

21

22 BY MR. STEPHENS:

23 Q. We're here today regarding inter partes review
24 proceeding IPR 2024-00226 involving U.S. patent 9118641.

25 Do you understand, Dr. Clark?

1 A. Yes.

2 Q. You understand that this deposition is being
3 transcribed, correct?

4 A. Yes.

5 Q. To ensure a clean record, I'll aim not to
6 interrupt you while you're speaking and answering my
7 questions.

8 Will you be able to do the same for me?

9 A. I think so, yes.

10 Q. If you need a break at any time, just let me
11 know. In general, I'll aim to break about every hour,
12 and we can take a lunch break as needed later in the
13 day. Okay?

14 A. Yeah. It's up to you. I don't need breaks,
15 but whenever you want one, take one.

16 Q. Sure. If you happen to need one, just let me
17 know.

18 And you indicated before we went on the record
19 that you'd received our binder with electronic copies of
20 documents from the record in the IPR, correct?

21 A. Yes. I put those in the dedicated folder for
22 the duration of this dep.

23 Q. Do you have any other copies of documents with
24 you?

25 A. No. As I said, it's a dedicated window. I

1 shut down those.

2 Q. Okay. Are you in communication with anyone at
3 this time outside of the dedicated window?

4 A. No, sir.

5 Q. Can you please state your full name for the
6 record?

7 A. Paul Christopher Clark.

8 Q. And please state your city of residence.

9 A. Bethesda, Maryland.

10 Q. You understand that you are under oath today?

11 A. I do.

12 Q. Is there any reason that you cannot give
13 truthful and accurate testimony today?

14 A. No.

15 Q. For clarity, I'll define several terms that
16 will be used throughout the questioning today. When I
17 use the terms "Petitioner" or "Datavant," I am referring
18 to Datavant, Inc.

19 Do you understand?

20 A. Yes.

21 Q. And when I use the terms "patent owner" or
22 "Vigilytics," I'm referring to Vigilytics LLC.

23 Do you understand?

24 A. Yes.

25 Q. When I use the term "'641 patent," I'm

1 referring to the patent that's been marked as
2 Exhibit 1001 in this proceeding. That's U.S. patent
3 9118641.

4 Do you understand?

5 A. I do.

6 Q. When I use the phrase "this IPR" or "this
7 proceeding," I'm referring to the inter partes review
8 proceeding, IPR 2024-00226.

9 Do you understand?

10 A. Yes.

11 Q. When I use the acronym POSITA or POSA, I'm
12 referring to a person of ordinary skill in the art at
13 the time of the alleged invention.

14 Do you understand?

15 A. I do.

16 Q. I also might refer to a number of exhibits
17 through the course of the deposition. I'd just like to
18 index them for the record.

19 When I'm referring to "your declaration" or
20 "the declaration," I refer to -- I'm referring to
21 Exhibit 1003 in this proceeding.

22 Do you understand?

23 A. Yeah. They are labeled as such in the folder
24 you provided.

25 Q. Great.

1 When I refer to "Evenhaim," I'm referring to
2 Exhibit 1005.

3 Do you understand?

4 A. As I said, yes.

5 Q. And when I refer to "Settimi," I am referring
6 to Exhibit 1006.

7 Do you understand?

8 A. That's how it's labeled.

9 Q. When I refer to "Dick," I'm referring to
10 Exhibit 1007.

11 Do you understand?

12 A. That's the way it's labeled. As I said, all
13 of them are labeled that way.

14 Q. Almost done here.

15 And when I refer to "Murphy," I'm referring to
16 Exhibit 1009.

17 Do you understand?

18 A. As labeled, yes.

19 Q. Can you please describe how you prepared for
20 today's deposition?

21 A. I had a meeting with counsel over the course
22 of two days, and prior to that, I had reread the
23 references in my declaration.

24 Q. Did those meetings occur this week?

25 A. Yes.

1 Q. Approximately how much time did you spend
2 preparing for the deposition?

3 A. I don't know. Maybe 20 hours; maybe less.

4 Q. What documents did you review in preparation
5 for your deposition?

6 A. As I said, the references in my declaration
7 primarily.

8 Q. Is there any material that's not identified in
9 your declaration that you reviewed for today's
10 deposition?

11 A. Maybe, but not that I recall sitting here.

12 Q. Before this IPR, have you ever served as an
13 expert in any capacity for Datavant?

14 A. Not that I recall. It's not impossible, but
15 not that I recall.

16 Q. Have you ever done any consulting for Datavant
17 before this IPR?

18 A. No.

19 Q. Have you ever collaborated on research
20 projects with Datavant?

21 A. No.

22 Q. And have you ever worked with Datavant's
23 counsel before Venable?

24 A. Yes. I've worked with Venable, but not with
25 this particular attorney.

1 Q. In what capacity did you work with Venable?

2 A. As an expert.

3 Q. Do you recall if those matters were IPRs?

4 A. I do not. I don't think they were, but,
5 again, it's not impossible. I haven't worked with them
6 recently.

7 Q. Can you please describe the process by which
8 you prepared your declaration in this proceeding?

9 A. I reviewed the patent, file history, various
10 other documents. Went through references that I had,
11 looked at references that were provided to me, and then
12 put together, in a collaborative effort, the declaration
13 that's in front of you.

14 Q. Can you describe the nature of that
15 collaborative effort in preparing the declaration?

16 A. Like any expert you work with, just -- I
17 provided my opinions, and I wrote some stuff, and they
18 wrote some stuff. And you end up with a declaration.

19 Q. There are portions of the declarations that
20 were written by counsel rather than by you?

21 A. As I said, it's a collaborative effort, but
22 I'm certainly responsible for the contents of the
23 declaration.

24 Q. Approximately what percentage of the
25 declaration was drafted by counsel?

1 A. I don't know.

2 Q. You don't recall?

3 A. Nope.

4 Q. If you had to put your best estimate on it,
5 how much do you believe was drafted by counsel?

6 A. I don't have an estimate for you. I'm not
7 going to guess.

8 Q. Approximately when did you begin working on
9 your declaration?

10 A. Several months ago.

11 Q. Is there a timeframe that you're able to
12 provide?

13 A. Not from memory, no.

14 Q. Apart from counsel, did you have anyone, such
15 as an assistant, help you with your declaration?

16 A. No.

17 Q. On page 7 of the declaration -- that's
18 Exhibit 1003 -- you provided a list of documents that
19 you indicated had been considered in forming your
20 opinions in the declaration, correct?

21 A. That's what it says, yes.

22 Q. Were there any other documents that are not
23 identified in this table that you considered in forming
24 your opinions?

25 A. My experience. All the documents that I've

1 read in this field all make up my background. So, yes,
2 I'm sure there's a whole bunch of them.

3 Q. Were there any specific documents that you
4 recall reviewing while preparing this declaration?

5 A. I see the Kerberos one that you provided.
6 That one came to mind immediately.

7 Q. Do you currently have any opinions regarding
8 the '641 patent that are not contained in your
9 declaration?

10 A. Not -- not that I'm aware of. I'm sure we're
11 going to explore that, though.

12 Q. Have any of your opinions that are stated in
13 the declaration changed since the time that you
14 submitted the declaration?

15 A. Not that I'm aware.

16 Q. And are you currently aware of any errors that
17 exist in your declaration?

18 A. Not that I'm aware.

19 Q. Similarly, are you aware of any typos in your
20 declaration?

21 A. I didn't read it necessarily for typos, but
22 any that I caught, I would have remedied.

23 Q. In your career, approximately how many times
24 have you been retained as an expert in litigation
25 matters?

1 A. Going back to 1995, probably 25 times. I
2 don't know. I think you have the case list for the last
3 five or ten years.

4 Q. Would you say more than two dozen times?

5 A. No. More than 25 times.

6 Q. More than 25 times.

7 And do you know approximately how many IPRs
8 you've been involved with?

9 A. Maybe ten. Probably a few more than that.

10 Q. You've been deposed in the past, correct?

11 A. Yes.

12 Q. Approximately how many times have you been
13 deposed?

14 A. A couple of dozen, probably.

15 Q. In your declaration at paragraph 2, you
16 indicated that you're being compensated for your time at
17 your normal consulting rate of 590 an hour?

18 A. That's correct.

19 Q. And is that still the case, you're being
20 compensated at that rate?

21 A. Yes.

22 Q. Is your compensation for your work on this
23 case in any way contingent on any factor other than the
24 number of hours in which you work on the case?

25 A. Of course not.

1 (Court reporter requested clarification.)

2 BY MR. STEPHENS:

3 Q. To your knowledge, has a Court ever precluded
4 you from offering an opinion?

5 A. No.

6 Q. To your knowledge, has a Court ever criticized
7 your opinions?

8 A. No.

9 Q. And, to your knowledge, has a Court ever
10 excluded your opinions?

11 A. No.

12 Q. All right. In the package that I sent, I
13 included Exhibit 1004, which is a copy of your
14 curriculum vitae.

15 Just let me know when you have that available.

16 A. I just brought it up.

17 Q. So I understand that you are the president and
18 CTO currently of SecureMethods Inc./Paul C. Clark LLC.
19 Is that correct?

20 A. That's correct.

21 Q. And you've held these positions since
22 July 1999?

23 A. Yes.

24 Q. And what are your responsibilities in these
25 roles?

1 A. I basically run the company. It's a sole prop
2 LLC currently, and so I'm responsible for day-to-day
3 operations.

4 Q. Do you -- have you worked with other
5 companies -- I'm sorry.

6 Have you been employed by other companies
7 during this timeframe?

8 A. Yes, I'm the CEO of Clear Guide Medical for
9 the last six or seven years.

10 Q. And that's not identified on the CV, correct?

11 A. It's not relevant.

12 Q. What does your work at Clear Guide Medical
13 involve?

14 A. I'm the CEO, and we do AI-guided medical
15 procedures. We have a suite of products that address
16 that issue.

17 Q. Can you elaborate a little bit on that work,
18 what the AI entails?

19 A. Yeah. You do instrument recognition and
20 targeting and use the computer to guide the clinician
21 onto the target with whatever the instrument is.

22 Q. Apart from Clear Guide Medical, are there any
23 other companies that you're employed by?

24 A. Not as an employee, no.

25 Q. And from January 1995 to July 1999, I

1 understand that you were the chief scientist at DynCorp
2 network solutions. Is that correct?

3 A. That's correct.

4 Q. What were your responsibilities in that role?

5 A. I was essentially the chief technical person
6 for that division of DynCorp.

7 Q. Did your -- can you describe the nature of the
8 projects that you worked on at DynCorp?

9 A. Yeah. They were security-related projects for
10 primarily government and DOD customers, some commercial.

11 Q. At DynCorp, were you ever involved in the
12 design or implementation of a HIPPA-compliant medical
13 record system?

14 A. Well, this was while HIPAA was being
15 developed, so I was involved with the policy people, and
16 we did secure databases. So, yes, we did data filtering
17 and de-identification of sensitive data. So the answer
18 is yes.

19 Specifically for medical, we had some work
20 with a healthcare client that involved, again,
21 controlling access to PII, so the answer would be yes.

22 Q. And was that specifically in relation to your
23 work at DynCorp?

24 A. Yes.

25 Q. Have you been involved in the design or

1 implementation of a HIPAA-compliant medical record
2 system at any other point during your -- during your
3 career?

4 A. At -- SecureMethods had a healthcare client
5 that was concerned with protecting PII, so from a
6 technical perspective, yes.

7 Q. Who is SecureMethods?

8 A. SecureMethods is my company. I founded it.

9 Q. I'm sorry.

10 You said SecureMethods had a healthcare client
11 that was concerned with protecting PII?

12 A. Yes.

13 Q. And so in your work with that client, were you
14 involved with ensuring compliance with the HIPAA privacy
15 rule?

16 A. Not the policy aspects; the technical aspects.
17 So the answer is we did the de-identification and the
18 data security to be compliant with HIPAA, but we were
19 not the ones that evaluated it.

20 I think there's also -- in my publication
21 list, you'll find a paper that was published -- I think
22 dealing with HIPAA compliance again from a technical
23 perspective.

24 Q. Do you see that in the list in your CV?

25 A. Let me see if it's there.

1 No, it's not there. It was for a minor
2 conference. These other ones were larger publications.

3 Q. Would you have been a named author on that
4 paper?

5 A. Yes.

6 Q. Were there any co-authors that you recall on
7 the paper?

8 A. Yes. Probably the same ones listed on the
9 ACSAC paper that is on my CV.

10 Q. And do you have an understanding of what the
11 HIPAA privacy rule is?

12 A. Yes.

13 Q. Can you describe your understanding of the
14 HIPAA privacy rule?

15 A. That it guarantees individuals control over
16 access to their medical records and, to the extent they
17 haven't provided authorization, the PII must be
18 de-identified before it can be disseminated.

19 Q. And do you understand what covered entity is
20 under HIPAA?

21 A. I don't have a specific definition. But, yes,
22 I mean, I know what a covered entity is.

23 Q. In general, what's your understanding of a
24 covered entity?

25 A. The entities that are subject to the HIPAA

1 regulations.

2 Q. The entities that must comply with HIPAA?

3 A. Correct.

4 Q. What types of entities may be deemed covered
5 entities under HIPAA, in your experience?

6 A. Well, the guys with the money are the
7 insurance companies, obviously. They have the biggest
8 stake in it. But also research institutions, big pharma
9 all have an interest in being able to do data mining.

10 Q. If I use the term "covered entity" during my
11 questioning today, will you understand what I'm
12 referring to?

13 A. Yes.

14 Q. All right. Let's turn to paragraph 26 of your
15 declaration, please.

16 A. Which paragraph again, sorry?

17 Q. Paragraph 26.

18 A. I'm there.

19 Q. And this starts a section in your declaration
20 related to claim construction; is that correct?

21 A. Yes.

22 Q. You state that, "I applied the term's ordinary
23 and customary meaning in accordance with my
24 understanding of how a POSA would understand them in
25 July of 2009," correct?

1 A. That's what it says.

2 Q. And then in paragraph 28, you indicated that,
3 with respect to certain terms, you'd adopted patent
4 owners' claim constructions from a litigation involving
5 the '641 patent in Massachusetts; is that correct?

6 A. Yep. That's what it says.

7 Q. These terms include "token," "server,"
8 "similarly encrypted," and "medical information" that
9 characterizes the group, correct?

10 A. Yes.

11 Q. And based on your review of these terms, do
12 you agree that they are the correct constructions?

13 A. No. They are just the ones that I use. I
14 mean, you apply the constructions that the Court or the
15 attorneys or whatever analyses you need to provide is,
16 and my agreement or disagreement doesn't matter.

17 Q. Have you formed an opinion as to whether you
18 agree or disagree with these constructions?

19 A. No, but I just apply them.

20 Q. Did counsel for the Petitioner ask you to
21 apply these constructions?

22 A. Yes.

23 Q. Just like to go through these individually.

24 The construction that you adopted for token
25 was "an identifier associated with an individual that

1 does not reveal the identity of the individual,"
2 correct?

3 A. That's what it says.

4 Q. Do you have any reason to believe that that
5 construction is incorrect?

6 A. Again, it doesn't matter. I don't have an
7 opinion on whether they are correct or not. I simply
8 apply them.

9 Q. You reviewed the specification and file
10 history of the '641 patent, correct?

11 A. That is correct.

12 Q. Is the construction that's provided in your
13 declaration for a token consistent with the use of token
14 in the '641 patent?

15 A. I mean, I think so. Again, I haven't done
16 that analysis. I haven't seen anything that directly
17 contradicts it.

18 Q. And as to a server, you adopted the
19 construction of a computer with a processor and memory
20 on a network that provides information in response to
21 requests from another computer, correct?

22 A. That's what I used.

23 Q. Is this construction consistent with your
24 understanding of the term "server" in the '641 patent?

25 A. As I said, I haven't seen anything to

1 contradict that. I mean, it might be slightly broader,
2 but it doesn't matter.

3 Q. And then as to similarly encrypted, the
4 adopted construction is, "Generated such that tokens
5 generated from corresponding information can be compared
6 to one another to detect a match," correct?

7 A. Yes.

8 Q. Based on your review of the '641 patent, is
9 this construction consistent with the specification and
10 file history of the patent?

11 A. Again, I haven't seen anything that
12 contradicts that. And in order for the systems to work,
13 it would need to work that way.

14 Q. And then similarly with respect to medical
15 information that characterizes a group, is the adopted
16 construction consistent with your understanding of that
17 term from review of the '641 specification and file
18 history?

19 A. Well, it's plain and ordinary meaning, so I
20 would assume that to be consistent.

21 Q. And then in the final bullet under
22 paragraph 28, you indicated that, "A POSA would
23 understand the foregoing construction of token to
24 encompass encrypted identifying information, which is
25 stated by the '641 patent," correct?

1 A. Yeah, that's one of the ways you could create
2 a token.

3 Q. And what prompted you to add this
4 clarification as to the meaning of token?

5 A. I was probably asked the question by the
6 attorneys.

7 Q. I'll refer to Claim 1 of the '641 patent,
8 Exhibit 1001.

9 A. Okay. I'm there.

10 Q. And under the producing step -- do you see, at
11 line 30, "producing"?

12 A. Yes.

13 Q. And the claim language recites, "Producing, by
14 processor of an encryption server, tokens wherein the
15 identity of the individuals in the group is unattainable
16 from the tokens," correct?

17 A. Yes.

18 Q. What does it mean, in your view, for the
19 identity of the individuals in the group to be
20 unattainable from the tokens?

21 A. Computationally infeasible to attain.

22 Q. Can you elaborate? What does computationally
23 infeasible mean?

24 A. It means it would take a computer too long to
25 figure it out.

1 Q. So would a hash -- would a one-way hash be an
2 example of a token?

3 A. Depends on the hash. But, I mean, that's a
4 one-way encryption.

5 Q. And what would -- what factors would you
6 consider to know if the hash -- whether the identity of
7 the individuals in the group would be unattainable from
8 a hash?

9 A. Whether it was computationally infeasible to
10 derive them.

11 Q. Does that mean computationally infeasible to
12 recover the original value that was hashed?

13 A. Without keying in -- or additional
14 information, yes.

15 Q. Are there any other factors that you would
16 consider to know whether the identity of individuals in
17 the group is unattainable from the tokens?

18 A. That's a pretty broad question. But within
19 the scope of the patent where we're talking about
20 encrypted information, I would understand that
21 unattainable to be cryptographically unattainable, which
22 means computationally infeasible to brute force.

23 Q. Okay. Let's turn to Exhibit 1005. Evenhaim.

24 A. Okay.

25 Q. You're familiar with the Evenhaim records,

1 correct?

2 A. Yes.

3 Q. Did you review Evenhaim while preparing your
4 declaration in this proceeding?

5 A. Yes.

6 Q. And have you read Evenhaim in its entirety?

7 A. Yes.

8 Q. How did you first encounter the Evenhaim
9 reference?

10 A. It was provided to me.

11 Q. Do you recall if you were aware of Evenhaim
12 before your involvement in this IPR?

13 A. I don't recall. I've been involved in a
14 couple of other de-identification matters, so it's
15 possible that I've seen it.

16 Q. Do you believe you have a good understanding
17 of the technology described in Evenhaim?

18 A. Yes.

19 Q. Is there any reason that you would not be able
20 to explain the technology described in Evenhaim in
21 response to my questions?

22 A. No, but we'll find out.

23 Q. All right. Let's turn to figures 4 -- I'm
24 sorry. Figures 4 and 4A of Evenhaim.

25 A. Okay.

1 Q. Just let me know when you're there.

2 A. I am.

3 Q. And Figure 4 shows representations of
4 computing systems operated by a pharmaceutical company,
5 Crossix, and health plan/pharmacy benefit managers,
6 correct?

7 A. Yes.

8 Q. Figure 4A then shows representations of
9 computing systems operated by a data consumer entity, a
10 data aggregator, and data source entities, correct?

11 MR. OLIVER: Objection. Form.

12 THE WITNESS: I mean, I see those things in
13 4B, yes. Or 4A, sorry.

14 BY MR. STEPHENS:

15 Q. Do you understand the health plan or PBM
16 entity shown in Figure 4 to be examples of data source
17 entities?

18 A. I mean, they could be. They could also be
19 consumers.

20 Q. Are they -- are they described in Evenhaim as
21 consumers?

22 A. I don't have complete recollection. Evenhaim
23 describes lots of different embodiments.

24 Q. What is a data source entity in Evenhaim?

25 A. An example of such an entity might be a

1 doctor's office or hospital or something like that.

2 Q. And data source entities can maintain
3 identifiable patient-level microdata?

4 A. They can.

5 Q. A data source entity would be responsible for
6 complying with HIPAA, correct?

7 A. Yes, they have to protect the PII.

8 Q. So they would be covered entities under HIPAA?

9 A. That would be my understanding.

10 Q. And then why is it important that the data
11 source entities not release private medical information
12 of individuals without their authorization?

13 A. That's what the law tells them to do.

14 Q. Would you agree that the pharmaceutical
15 company depicted in Figure 4 is an example of a data
16 consumer entity?

17 A. You're talking about the pharmaceutical
18 entity?

19 Q. On the left-hand side, that's right.
20 Pharmaceutical company.

21 A. Yes. I mean, again, they may come into
22 possession of PII as well. But in this example, they're
23 one of the consumers.

24 Q. And what is a data consumer entity in
25 Evenhaim?

1 A. It's somebody who is attempting to search the
2 patient data.

3 Q. And a data consumer entity is not necessarily
4 a covered entity under HIPAA, correct?

5 A. To the extent they don't have -- to the extent
6 they don't have access to PII, they are not.

7 Q. In Figure 4, the Crossix system shown in the
8 center of the figure is an example of a data aggregator
9 in Evenhaim, correct?

10 A. Yes.

11 Q. What is a data aggregator?

12 A. It's functionally a database server, DDMS,
13 that also includes encryption and token matching
14 capabilities.

15 Q. And the data aggregator is not necessarily the
16 covered entity under HIPAA, correct?

17 MR. OLIVER: Objection. Form.

18 THE WITNESS: No, it could be. I mean, if it
19 has access to the PII -- again, it depends on how the
20 databases are architected. But if it -- if it has
21 access to the PII, it's covered.

22 BY MR. STEPHENS:

23 Q. Are you aware of any disclosure in Evenhaim
24 where the data aggregator has access to PII?

25 A. I don't have complete recollection, but I

1 believe that it's constructing tokens in some of the
2 embodiments. So, yes, it would need access to the PII
3 in order to access or create those tokens.

4 Q. Are you aware of any disclosure in Evenhaim
5 where the data aggregator has access to PII correlated
6 with that individual's medical data?

7 A. Yes. I mean, one of the examples, they're
8 encrypting, you know, patient lists, like I see in
9 Number 3. And that's certainly PII.

10 Q. And in that example, the patient lists don't
11 contain the patients' medical data, correct?

12 A. They may or may not have access to the data.
13 Again, Evenhaim provides lots of possibilities.

14 Q. Is there -- are you able to identify any
15 disclosure in Evenhaim where the patient lists would
16 have -- would include medical data of the patients on
17 the list?

18 A. I -- I would have to read the entire
19 reference. I'll do so if you wish, but I know that one
20 of skill in the art would understand that one possible
21 implementation of this would have the Crossix server
22 accessing PII.

23 Q. I'd invite you to review the specification and
24 let me know if you see any examples where the data
25 aggregator does have a patient list that includes the

1 patients' medical data.

2 A. At least in Figure 5, it says, (as read)
3 "Analyze all patient records on the patient ID list," so
4 that would include the medical data from my perspective.

5 Q. And in Figure 5, that's a box shown within the
6 data cruncher module, correct?

7 A. Yes.

8 Q. And the data cruncher module is part of the
9 data source entity rather than the data aggregator,
10 correct?

11 A. I think it could be implemented either place.
12 Again, it depends on how the database is architected.
13 This reflects one embodiment, but you could certainly
14 put it anywhere.

15 Q. Are you able to identify any disclosure in
16 Evenhaim where the data cruncher module is located at
17 the data aggregator?

18 A. Well, it -- again, Evenhaim provides several
19 embodiments, some of which have PII processing on the
20 aggregator and some of them which don't.

21 Q. So there's no disclosure of the data cruncher
22 module being part of the data aggregator, correct?

23 A. It would -- those functions would necessarily
24 need to occur on the aggregator, depending upon the
25 architecture of the database. Evenhaim is just telling

1 you the things that need to happen and potential places
2 where they could happen.

3 Q. But there's no basis for -- in Evenhaim itself
4 in which it's disclosed that the data cruncher module is
5 located on the data aggregator, correct?

6 A. No, that's not correct.

7 Q. Are you able to identify a disclosure where
8 the data cruncher module is located on the data
9 aggregator?

10 A. We can find a disclosure of an embodiment in
11 which the PII is on the aggregator, in which case the
12 data cruncher functions would have to be performed
13 there, as I've explained.

14 Q. You said that "we can find," but I'm waiting
15 for it to be found.

16 Is there an example that you can point me to?

17 A. Is there an -- you want me to go through and
18 find where PII is processed on the data aggregator?
19 We've already done that.

20 Q. Where the data cruncher module is located on
21 the data aggregator.

22 A. I'm not --

23 Q. Why don't you -- we don't -- if you're not
24 able to point to any disclosure, that's fine. We can
25 move on. I'm just -- I'd like to be sure for the

1 record.

2 A. Well, for the record -- which I'm explaining
3 to you. I understand what you're trying to do.

4 But for the record, the figures are particular
5 embodiments. And so the disclosure, the written text,
6 talks about the processing of PII on the aggregator, and
7 that would necessarily require those cruncher functions,
8 in whole or in part, to be on that aggregator by the
9 disclosure in text. They are not shown in the figures.

10 Q. I appreciate your position, Dr. Clark.

11 I'm looking for any specific examples in
12 Evenhaim where the data aggregator has PII along with
13 the patient's medical data.

14 Are you able to identify any specific
15 examples?

16 A. And you want that to be on the aggregator?

17 Q. On the aggregator, correct.

18 A. All right. So sit back and relax.

19 Well, we can start with the abstract. Says,
20 "Between a secure aggregator" -- and it needs to be
21 secure if it has PII -- "and" -- conjunctive -- "sources
22 having respective access to privacy-sensitive
23 microdata."

24 So in that case, the PII is on the aggregator.

25 Q. And are there any examples of the patient list

1 processed by the aggregator, including medical data?

2 A. It says --

3 MR. STEPHENS: Object to form.

4 THE WITNESS: It says, "Privacy-sensitive
5 microdata." I understand that to include PII and
6 medical data. I mean, that's the subject of the
7 reference.

8 BY MR. STEPHENS:

9 Q. And what is your understanding of what the
10 data aggregator does with the patient list?

11 A. It depends on the particular embodiment. In
12 general, it's gonna use it to facilitate the searching
13 of the sensitive data.

14 Q. So it would send the patient list to the data
15 source entities; is that correct?

16 A. That's one way it could do it.

17 Q. Are there other ways that you have in mind
18 that it can do it?

19 A. Yes. As I said, it can create the tokens and
20 search for tokens in the database. It has -- it has to
21 be secured because it has access to the PII.

22 Q. Let's turn back to Figure 4.

23 And there are a series of steps shown in this
24 figure, 1 through 7, correct?

25 A. Yes.

1 Q. Can you describe your understanding of what
2 happens at each of these steps?

3 A. This is one particular embodiment. Is there
4 any in particular that you're interested in, or you want
5 me to talk through all of them?

6 Q. In the embodiment that's shown in Figure 4.

7 A. All right. So you have a pharmaceutical
8 company attempting to access covered entities using the
9 Crossix server, and so it sends a request using the user
10 interface provided by the Crossix server.

11 And the Crossix server generates the query to
12 one or more databases and then aggregates the results --
13 makes sure, presumably, that they don't have PII in
14 them -- and then sends it back for final analysis to the
15 requester.

16 Q. And so in the operations shown in Figure 4, we
17 have data being transmitted between the data aggregator
18 and the data source entities, correct?

19 A. Well, yes, they're the -- they have the
20 patient-level microdata, as it says.

21 Q. And this data could be transmitted over
22 communication networks, correct?

23 A. It depends on the particular implementation.
24 You would seek not to let that PII escape past your
25 security boundary.

1 Q. What do you mean by "security boundary"?

2 A. Well, the Crossix server is the security
3 boundary between the requester, to the extent they are
4 not sending PII back, and the sensitive data.

5 Q. The requester, is that a pharmaceutical
6 company in Figure 4?

7 A. Yes.

8 Q. At Column 13 of Evenhaim at lines 33 to 36,
9 Evenhaim discloses that, "Every step requiring a
10 transmitting of data (or of at least one file) and every
11 respective associated step requiring receiving of that
12 data (or of that at least one file) may preferably
13 include respective encryption and decryption."

14 Did I read that correctly?

15 A. That's what it says.

16 Q. And further down that paragraph, Evenhaim
17 discloses that it's "generally preferable to include
18 some degree of data transmission security," correct?

19 A. That's what it says.

20 Q. Do you have an understanding of data
21 transmission security?

22 A. Sure.

23 Q. What is data transmission security?

24 A. You're going to prevent unauthorized
25 disclosure, integrity violations, those sorts of things.

1 Q. What do you mean by "unauthorized disclosure"
2 and "integrity violations"?

3 A. Those are terms of art. I mean, you don't
4 want the data modified, and you don't want unauthorized
5 people seeing the data.

6 Q. And so encryption would be one way to provide
7 data transmission security?

8 A. Encryption will prevent unauthorized
9 disclosure.

10 Q. And with regard to data integrity, what can
11 you do to provide data transmission security?

12 A. Hashes are one way to do that. Keyed hashes
13 or message authentication codes are another way to do
14 that. There are entire books on ways to implement those
15 schemes.

16 Q. Are you familiar with any data transmission
17 security schemes from the early 2000s?

18 A. Sure. Endless numbers. SSL being one to
19 provide streaming-level security. There's also -- were
20 protocols like S-HTTP, S/MIME, all sorts of ways.

21 Q. Have any of those ever been applied in
22 Evenhaim to provide the data transmission security?

23 A. I'm sure they were used -- intent on using
24 standard algorithms. It looks like they had their own
25 protocol, however. They may have used that in

1 conjunction with other countermeasures, like I said,
2 SSL, that existed to protect maybe the queries that were
3 coming across.

4 Q. How is a message typically encrypted for data
5 transmission security?

6 A. It depends on the implementation. As I said,
7 there are any number of ways to do it.

8 Q. Are there -- would you typically need an
9 encryption key for an encryption scheme?

10 A. If you're going to encrypt something, there's
11 a protocol that needs to go with that that includes an
12 algorithm, key management, all sorts of things.

13 Q. And can you just briefly describe. What is an
14 encryption key?

15 A. It is a string of bits that's fed into an
16 algorithm along with the data stream to produce a cipher
17 text.

18 Q. And if you're encrypting a message for
19 transmission over a network, do you encrypt the entire
20 message at a time?

21 A. Not necessarily. It depends. I mean, some
22 systems will actually use some form of super encryption
23 where you have multiple layers of encryption. So,
24 again, it depends on the implementation.

25 Q. If -- I guess, for super encryption, does that

1 mean you apply first kind of encryption to the message
2 and then re-encrypt it?

3 A. It would mean that interior portions of the
4 data are encrypted in addition to what you're focused
5 on, which is streaming, like SSL-level encryption.
6 Those are not incompatible.

7 Q. At Column 14, lines 3 to 4, Evenhaim notes
8 that he's "returning to the abovementioned aspects of
9 preferable encryption."

10 Do you see that?

11 A. Yes.

12 Q. And so that refers, again, to the description
13 that we just went over in Column 13 about it being
14 preferable to include some degree of data communication
15 security, correct?

16 MR. OLIVER: Objection. Assumes facts.

17 (Court reporter requested clarification.)

18 THE WITNESS: Yeah. I mean, as I said,
19 there's any number of encryption schemes available to
20 protect data in different ways and at different levels
21 of security.

22 So as I said, you can secure the channel and
23 secure specific fields or items of data that you need to
24 secure. And, again, that's dictated by policy. One of
25 skill in the art would know that all of these were

1 available.

2 BY MR. STEPHENS:

3 Q. These are all schemes that would apply for
4 data transmission security, correct?

5 A. Well, you're going to provide data security,
6 and then if you choose to send it over a network, that
7 may require something else. So that -- there's not a
8 one size fits all.

9 Q. Can you elaborate on that? It requires
10 security, and then if you send it over a network, that
11 requires something else. Are there two different things
12 there?

13 A. Sure.

14 I may secure the data on my server in various
15 ways, including encryption, de-identification. And then
16 I may also secure the channel once that data is being
17 sent over the network so that I can protect, for
18 instance, the contents of the query as well as the
19 results.

20 And so it's quite possible to have a situation
21 in which super encryption is occurring.

22 Q. In that paragraph at Column 14 at lines 4 to
23 7, Evenhaim notes that it's "certainly strongly advised
24 that, regardless of the general level of encryption
25 elected, a parameter list including 'individuals' should

1 carry a stronger level of encryption," correct?

2 A. That's what it says.

3 Q. Why would a stronger level of encryption apply
4 to a parameter list that includes individuals?

5 A. As I said, you may wish to encrypt things one
6 or more times or with different keys depending upon the
7 level of protection you wish to provide. One -- anyone
8 implementing one of these systems would know that.

9 Q. All right. Let's look back at Figure 4, if
10 you would.

11 A. Okay.

12 Q. At Step 3 in Figure 4, the Crossix system is
13 set to encrypt patient list and query, correct?

14 A. That's what it says.

15 Q. Do you agree that the query is encrypted at
16 Step 3 to provide data transmission security?

17 A. Maybe; maybe not.

18 Q. Do you have an opinion?

19 A. Yeah, maybe or maybe not. It depends. I
20 mean, this is a schematic of one embodiment. So, I
21 mean, the motivation for encrypting that could be any
22 number of things.

23 Q. In light of the disclosure that we read at
24 Column 13 that it's generally preferable to provide data
25 transmission security, would a person of skill in the

1 art reading Figure 4 understand that the query is
2 encrypted to provide data transmission security?

3 A. No, not necessarily. The query could be
4 encrypted because that's how it's going to match fields
5 in the database. I mean, it depends on how the system
6 is designed.

7 Q. And I'm not asking about the patient list
8 right now. I'm asking about the query specifically.

9 So it's my understanding that the query does
10 not include fields that would be matched in the
11 database. Is that correct?

12 A. No. The query may very well include fields
13 that would be matched.

14 Q. Is there a portion of Evenhaim that you are
15 referring to for your understanding of the query?

16 A. The query is a term of art that refers to a
17 database query. The standard for database queries is
18 called SQL, and it includes things like "select from
19 where," where "where" is your conditions and your query.

20 And if you need to match those, then it's
21 possible that you would need to encrypt them in order to
22 match them.

23 Q. What is a patient list as referred to in
24 Step 3 of Figure 4?

25 A. I would understand it to be a list of patients

1 and identifiers.

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.

11 Q. Let's look at Figure 5, please.

12 A. Okay.

13 Q. And within the data cruncher module, towards
14 the top right of that module, there's a box that says,
15 "Decrypt patient identifier list HP(i,j)."

16 Do you see that?

17 A. I do.

18 Q. Would you agree that, in Figure 5, each
19 patient identifier list is decrypted separately from the
20 other lists?

21 MR. OLIVER: Objection. Form. Foundation.

22 THE WITNESS: Yeah. I'm not sure I read that
23 much into it. I take it at face value. It says, (as
24 read) "Decrypt the patient identifier list."

25 That's a pretty broad function.

1 BY MR. STEPHENS:

2 Q. There are multiple patient identifier lists
3 referenced in Figure 5, correct?

4 A. I mean, it does use plural. It allows for one
5 or more patient lists, so I'm sure.

6 Q. What is your understanding of HP(i,j)?

7 A. It's a patient identifier.

8 Q. HP(i,j), that's referring to patient
9 identifiers?

10 A. It is a particular patient identifier.

11 MR. STEPHENS: All right. We've been going
12 for a bit over an hour. Would you like to take a -- I
13 would actually appreciate it. Could we take a
14 five-minute break?

15 THE WITNESS: Yes, that's fine. Let's make it
16 a little bit longer, but, yes.

17 MR. STEPHENS: Ten minutes?

18 THE WITNESS: Fine.

19 MR. STEPHENS: Okay. Thanks.

20 (Recess: 10:50 a.m. to 11:04 a.m.)

21 BY MR. STEPHENS:

22 Q. Dr. Clark, during our break, did you discuss
23 the substance of your testimony at all with counsel?

24 A. I didn't discuss it with anyone.

25 Q. Let's turn to Column 12, please, of Evenhaim.

1 Let me know when you're there.

2 A. I'm there.

3 Q. And in the paragraph that begins with "a
4 further class of embodiments," Evenhaim refers to
5 "interim data merger enabled embodiments," correct?

6 A. Yes.

7 Q. And then at line -- starting at line 12,
8 Evenhaim discloses, "If the data sources are careful to
9 encrypt the identifying portions of each record using a
10 common encryption 'key,' then further down the data
11 processing circuit, it will be possible to link records
12 related to a common individual without compromising the
13 identity of that individual."

14 Did I read that correctly?

15 A. What it says.

16 Q. The mention of data sources at line 13 can
17 refer to the data source entities, correct?

18 A. I think it could, sure.

19 Q. Would you understand that multiple data
20 sources can produce the same encrypted identifier for an
21 individual by using a common encryption key?

22 A. That's not necessarily the way that I would
23 implement it. But, I mean, that's what it says for this
24 embodiment.

25 Q. And in this embodiment, the data aggregator is

1 the entity that would be further down the data
2 processing circuit, correct?

3 MR. OLIVER: Objection. Form.

4 THE WITNESS: That would be one place you
5 could do it. As I said, the functions could be anywhere
6 on that side of the security boundary.

7 BY MR. STEPHENS:

8 Q. And so the data aggregator can link records
9 related to a common individual, correct?

10 A. Using encrypted identifiers, yes. I mean, for
11 this embodiment.

12 Q. Okay. So if the individual had two or more
13 records with the same encrypted identifier, the data
14 aggregator would be able to correlate them and determine
15 that they pertain to the same person, correct?

16 A. Well, the ID would match. So then the
17 aggregator can do whatever it wants to do with that
18 information, but it would know -- or reasonably know
19 that that was the same individual.

20 Q. Then at line 16, again in Column 12, Evenhaim
21 discloses that, "Special care must be taken that the
22 entity performing the linkage is not capable of knowing
23 the key and decryption function because knowing these
24 facets would enable a breach of the individual's
25 privacy," correct?

1 A. That's what it says for that embodiment, yes.

2 Q. How would knowing the key and decryption
3 function allow the entity that performs the linkage to
4 breach the individual's privacy?

5 A. It could decrypt the identifiers.

6 Q. And by decrypting the identifiers, how would
7 that breach the individual's privacy?

8 A. If the identifier contains PII, then it would
9 be covered by HIPAA.

10 Q. Further down in Column 12 at line 26, Evenhaim
11 discloses that, "There are numerous locations where an
12 encryption of individual identification and/or merger of
13 data for individuals could be facilitated."

14 Do you see that?

15 A. Yes.

16 Q. Evenhaim notes that encryption or merger can
17 occur on the aggregator processor side or the
18 source-entity processor's side; is that correct?

19 A. Yeah. As we've been discussing, those
20 functions can be formed -- or be performed any number of
21 places on that side of the security boundary.

22 Q. When you say "on that side of the security
23 boundary," what's encompassed on that side of the
24 security boundary?

25 A. Access to PII, as we've been discussing, can

1 occur on the aggregator and on the data sources. So
2 depending upon how the system is architected, it's
3 necessary to protect that information to comply with the
4 law.

5 Q. So what entities do you consider to be within
6 the same security boundary?

7 A. Well, anybody who has access to the PII.
8 That's what we're trying to secure here.

9 Q. So who would those entities be in Evenhaim?

10 A. You already asked me that, but it would
11 typically be things like hospitals and doctors.

12 Q. Evenhaim discloses that the data source
13 entities provide de-identified data to the data
14 aggregator, correct?

15 A. That's one of the ways they could do it.

16 Q. And so in that case, the data source entities
17 and the data aggregator would not be within the same
18 security boundary; is that correct?

19 A. They would be at different levels of security,
20 but they would still have security requirements. So, I
21 mean, arguably, that would be different domains, but
22 they would still have security requirements placed upon
23 them.

24 Q. So is there a provision of HIPAA that you're
25 aware of in which an entity that only receives

1 de-identified data would be subject to the HIPAA privacy
2 rule?

3 A. If it only has access to de-identified data,
4 it's not covered. As we discussed, it's possible for
5 places like insurance companies to process both.

6 Q. One moment. I'm just gathering my notes here.

7 So am I correct in understanding from your
8 declaration that, in your view, Evenhaim's disclosure of
9 the data aggregator performing encryption supports an
10 understanding that Evenhaim's data sources would perform
11 what you call token matching to identify individual
12 patient records?

13 A. That's one possible way it could do it for
14 sure since it has an encryption capability. It could
15 de-identify the information before querying it if it
16 wanted to.

17 Q. I'm sorry, what would de-identify the data
18 before querying?

19 A. The aggregator certainly has the capability to
20 do so because it has encryption and decryption
21 functions.

22 Q. But the aggregator would not need to do so,
23 correct?

24 A. It depends on the design of the database.

25 Q. And the queries are --

1 I'm sorry, go ahead.

2 A. In order for the system to function, it's
3 going to have to create meaningful queries on fields
4 that can be matched. And those can be, as we've
5 discussed, matched on the aggregator, or they could be
6 matched at the data sources depending upon the fields
7 and the protocol that's being used.

8 Q. The queries are sent to the data source
9 entities, correct?

10 A. Yes.

11 Q. And the data source entities are covered
12 entities under HIPAA, correct?

13 A. Generally speaking, yes.

14 Q. And so the data source entities would,
15 themselves, maintain PII for patients, correct?

16 A. Well, that's sort of the point of the
17 reference, right?

18 Q. And so a query that's sent from a data
19 aggregator to a covered entity would not need to
20 de-identify patient data, correct?

21 A. It depends. As I said, the disclosure in the
22 embodiments in Evenhaim allow for both possibilities.

23 Q. So in the embodiments in which you say that
24 token matching would occur at the data source entities,
25 would the data sources encrypt PII using the same

1 encryption key as the data aggregator to produce
2 matching tokens?

3 A. Well, they would need to generate similar IDs
4 somehow. But certainly it's possible that the systems
5 that they would make available to the aggregator had
6 been de-identified from their internal sources. It's
7 not ruled out by the reference by any means.

8 Q. And so in those embodiments, again, would the
9 data sources be capable of determining the identities of
10 the individuals from the tokens it receives from the
11 data aggregator?

12 A. Again, it depends. The key management scheme
13 and everything else would play a role in what anybody
14 could access, but it's -- the reference allows for you
15 to create those tokens wherever you wish.

16 Q. If the data source entity maintained a record
17 that associated the patient's identity with a token and
18 then it received a matching token from the data
19 aggregator, would the data source entity be able to use
20 the token from the data aggregator to identify the
21 individual?

22 MR. OLIVER: Objection. Form.

23 THE WITNESS: I mean, anything is possible.
24 It depends on how the system is set up. If I were their
25 security consultant, I'd probably have some process

1 separation, but people do different things.

2 BY MR. STEPHENS:

3 Q. But there's no such process separation
4 disclosed in Evenhaim, correct?

5 A. It merely focuses on securing the PII and
6 various ways and places that you can do that.

7 Q. And, again, in these embodiments, would the
8 data sources return tokens with the de-identified
9 patient records to permit the aggregator to link records
10 to the same individual?

11 A. That's one possible way to do it, yes.

12 Q. Are there any specific examples in Evenhaim
13 that you can identify where the data sources match
14 tokens received from the data aggregator to
15 de-identified patient data?

16 A. I think we've already discussed some of those,
17 right, that the de-identification and, as you call it,
18 the crunching could occur on the source entity or at the
19 aggregator.

20 So in the cases where that occurred at the
21 source entity, then they would be sending back the
22 tokens to be linked by the aggregator.

23 Q. And I guess I'm not asking about the
24 identification.

25 I'm asking if there are any specific examples

1 that you can point to in Evenhaim where the data source
2 entities match a token received from the data aggregator
3 to a corresponding token maintained by the data source
4 entity?

5 A. If the tokenization occurs at the data source
6 entity, that's the way it would have to work for the
7 system to function. You can't match otherwise.

8 Q. But that's not expressly disclosed in
9 Evenhaim?

10 A. It is. That one of skill in the art would
11 know that, if that's storing tokens in the database at
12 the source entity, that that's the way it would have to
13 function. Otherwise you couldn't match.

14 Q. I'm not asking about what a person of skill in
15 the art would -- would or would not have known.

16 I'm asking if there's an express disclosure in
17 Evenhaim of matching performed at the data source
18 entities. Are you able to point to any?

19 A. Yes, they're storing the database, and in
20 order to query the database, you have to match. That's
21 the way the system has to function.

22 Q. So, again, you're saying what has to occur and
23 what a POSITA would understand.

24 I'm asking for specific examples expressly
25 disclosed in Evenhaim.

1 A. And I've answered that question about four or
2 five times now. I'll do it one more time.

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.

17 Q. There's no express disclosure of a token in
18 this portion, correct?

19 A. It doesn't use the word "token." It talks
20 about using privacy-identified fields and creating a
21 single unit. I would understand that to be a token.

22 I mean, if you're looking for the word
23 "token," it's not there, but we have an understanding of
24 what a token is by the construction.

25 Q. And this discussion pertains to alleged prior

1 art that's distinct from Evenhaim's present invention,
2 correct?

3 A. Not distinct necessarily. These are systems
4 that may need to be, in fact, supported by Evenhaim. So
5 it acknowledges that they exist.

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.

14 Q. All right. Let's turn to your declaration,
15 please.

16 A. Okay.

17 Q. And paragraph 40.
18 Are you there?

19 A. I am.

20 Q. And towards the bottom of page 20, in
21 paragraph 40, there's a sentence that says, "Aside from
22 the guidance in Figure 4, a POSA would also understand
23 that, in order to comply with HIPAA, the query sent from
24 the aggregator to the data sources should not include
25 personally identifying information."

1 Do you see that?

2 A. Yes. That's the case where the token is, in
3 fact, on the source entity.

4 Q. Are you aware of any provisions of HIPAA that
5 would be violated by a noncovered entity transmitting
6 PII to a covered entity?

7 A. I don't think the noncovered entity is allowed
8 to have the PII.

9 Q. And by "PII," I'm referring to patient names,
10 for example, decoupled from medical data.

11 A. Well, that's not what HIPAA defines it as.
12 It's personally identifiable information. So it's
13 information that allows you to deduce the identity of
14 the individual, and that's not just names. There are
15 other ways to do that.

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.

1 Q. Would you agree that the data aggregator in
2 Evenhaim can transmit a patient list to the data sources
3 without any medical information for the patients?

4 A. I'm sure that's possible. I mean, there's --
5 again, there's multiple embodiments disclosed in
6 Evenhaim.

7 Q. And there's no express disclosure in Evenhaim
8 of the data aggregator transmitting medical data to the
9 data sources, correct?

10 A. I don't know. I haven't searched for that. I
11 mean, it's certainly possible that it could. It would
12 depend upon the query that was generated. I mean, it
13 might -- I could imagine a situation where the patient
14 list in a particular medical procedure would be
15 transmitted.

16 Q. But, again, no express disclosure in Evenhaim
17 of that situation, correct?

18 A. I'm not sure that's true. I mean, we can sit
19 around and go search it again, but it's certainly the
20 possibility that's allowed for.

21 Q. Let's take a few minutes. If you could
22 identify any examples for me, that would be helpful.

23 A. Well, Figure 4 is showing a pharmaceutical
24 company that's looking for certain drugs associated with
25 certain names. So in that case, that would be part of

1 the query coming across.

2 Q. Can you point to that -- I'm sorry, that
3 portion of Figure 4 that you were referring to again?

4 A. The pharmaceutical company is requesting
5 information on patients and medications. So that would
6 be medical information associated with an individual.
7 That would be part of the query.

8 Q. So the query would identify the medications
9 that are of interest, correct?

10 A. And the individual.

11 Q. Correct.

12 But it does not identify that those
13 individuals have taken that medication, correct?

14 A. No, that's the query. So the Crossix server
15 is going to have to send that information when it's
16 querying the covered entities.

17 Q. And so are you saying that a query that
18 includes information about what medical information is
19 sought would be covered by HIPAA?

20 A. That's not what I said.

21 I'm answering your question, and your question
22 was provide an explicit disclosure where the patient
23 list and medical information would be part of the query.
24 And that's what I just gave you.

25 Q. And, yeah, I'm trying to understand this

1 example.

2 So with the medical information that you've
3 given in Figure 4, is that a type of information that
4 would require protections under HIPAA?

5 A. Yeah. If a -- if a person is taking a certain
6 medication, that's definitely protected by HIPAA.

7 Q. But the information about whether the patients
8 are taking the medications, that's not contained in the
9 query, correct?

10 A. It is going to be -- not whether they are.
11 The answer to the query is stored in the data source.

12 Q. Right.

13 So the query itself doesn't contain the
14 patient's medical data records, correct?

15 A. It's going to include medical data and then an
16 answer. So asking the question would necessarily
17 transmit the information about the medical data being
18 sought.

19 Q. But the query itself does not contain records
20 of the patient's medical history, correct?

21 A. No. The answer to the question does. And so
22 you asked for when medical information would be included
23 with the patient list. And that's the example.

24 Q. All right. I think I understand. Thank you.
25 Going back to your declaration, then, at

1 paragraph 42.

2 Let me know when you get there.

3 A. Okay.

4 I said okay.

5 Q. I'm sorry.

6 In this paragraph, you refer to an additional
7 level of security that could be added to the '641 patent
8 in Evenhaim; is that correct?

9 A. Sure.

10 Q. And can you describe this additional level of
11 security?

12 A. Yeah. I mean, as we've discussed, you can do
13 multiple levels of encryption if you wish, using
14 different keys and different tokens. It depends upon
15 the granularity of the system that you're trying to
16 provide.

17 Q. This additional level of security that you've
18 described in paragraph 42 is not described in Evenhaim
19 itself, correct?

20 A. I don't have complete recollection. It
21 certainly allows for it. I mean, as we've been
22 discussing, you can do things like super encryption. It
23 would depend upon the requirements of the system you had
24 built.

25 Q. You have no citations to Evenhaim in

1 paragraph 42; is that correct?

2 A. I don't see any.

3 Q. Are you aware of any disclosure in Evenhaim
4 that provides this additional level of security?

5 A. Well, it, as we've discussed, allows
6 encryption to occur at the data source and also at the
7 aggregator, so I would understand that to allow for
8 multiple encryptions.

9 Q. All right. Let's go forward to paragraph 86,
10 please.

11 Are you there?

12 A. Almost.

13 Okay. I'm there.

14 Q. So in this paragraph, you indicate that, in
15 the absence of token matching, there would be a need
16 for, quote, "repeated encrypting and decrypting of the
17 patient names. To comply with HIPAA" --

18 Do you see that?

19 A. Yes.

20 Q. Can you explain the basis for your statement
21 there?

22 A. I don't understand your question.

23 Q. Yeah. Why would there be a need for repeated
24 encrypting and decrypting?

25 A. Well, if you're going to have to create the

1 token every time the name comes across, then you would
2 repeatedly encrypt and decrypt in order to match.

3 Q. Could you avoid the repeated encryption and
4 decryption simply by not encrypting the individual
5 patient names and the request sent from the data
6 aggregator, apart from encryption of the message for
7 data transmission security?

8 MR. OLIVER: Objection. Form.

9 THE WITNESS: I mean, any -- anything is
10 possible. But I don't -- I think, if you're going to
11 match the tokens as we understand the term "token" to
12 mean, you're going to have to encrypt the PII and
13 decrypt.

14 BY MR. STEPHENS:

15 Q. Why would you have to decrypt? I'm sorry.
16 Can you clarify?

17 A. In order to match?

18 Q. Yes.

19 A. Because it depends on what's on the other side
20 of the database. If it is not storing tokens, then
21 you're going to have to match by name. Right? Or some
22 other PII.

23 Q. And is the problem of repeated encryption and
24 decryption disclosed anywhere in Evenhaim?

25 A. I -- I don't think it is specifically

1 disclosed there. It is just what one who was
2 implementing the system would understand.

3 MR. STEPHENS: All right. I am about ready to
4 transition to another reference. Maybe this would be a
5 good point for, say, a five-minute break.

6 THE WITNESS: If you wish. Yeah. I'd
7 probably do more like ten again, but that's fine.

8 MR. STEPHENS: Yeah, how about we reconvene at
9 noon Eastern.

10 THE WITNESS: Okay.

11 (Recess: 11:47 a.m. to 12:06 p.m.)

12 BY MR. STEPHENS:

13 Q. I'd like to turn to the Murphy reference,
14 which is Exhibit 1009.

15 Let me know when you have that document
16 available.

17 A. Just digging for it.

18 All right. Go ahead.

19 Q. You're familiar with Murphy, correct?

20 A. Yes.

21 Q. Did you review Murphy while preparing your
22 declaration?

23 A. Yes.

24 Q. Have you read Murphy in its entirety?

25 A. I've certainly scanned it. I'm not -- it's a

1 pretty long document, but I'm pretty sure I looked
2 through all of it, yeah.

3 Q. How did you first encounter the Murphy
4 reference?

5 A. It was provided by the attorneys.

6 Q. To the best of your recollection, were you
7 aware of Murphy before your involvement in the present
8 proceeding?

9 A. I don't think so. I was looking at the
10 conference to see if it was one that I attended, but I
11 don't think it was.

12 Q. Do you believe you have a good understanding
13 of the technology described in Murphy?

14 A. A reasonable understanding. I mean, it was
15 used for one particular claim limitation, so -- but I'll
16 be happy to answer whatever questions you have.

17 Q. All right. Yeah. Let's turn to page 555 of
18 Murphy.

19 Are you there?

20 A. I am.

21 Q. All right. I'll have some questions about the
22 discussion on page 555. If you'd like to take a moment
23 to review, please feel free.

24 A. Okay.

25 Okay.

1 Q. And so Murphy describes a query tool, correct?

2 A. Yeah. A query tool for examining
3 de-identified information.

4 Q. And in this section on page 555, Murphy
5 describes a desire to obfuscate the results provided by
6 the query tool, correct?

7 A. Right. It does -- it doesn't want you to be
8 able to zero in on one particular individual.

9 Q. And so the result that Murphy's query tool
10 provides is a number of patients that satisfy the
11 parameters in a search request; is that correct?

12 MR. OLIVER: Objection. Form.

13 THE WITNESS: Well, in particular, it's not
14 gonna return with less than three records is the
15 limitation so that the repeated queries don't allow you
16 to single out one individual or two individuals from
17 which you could determine the PII they say.

18 BY MR. STEPHENS:

19 Q. In the last paragraph on the left-hand side --
20 Excuse me. I'm going to take a drink of
21 water, if that's all right.

22 All right. I'll restart my question.

23 In the last paragraph on page 55 [sic] on the
24 left-hand column, beginning "one [sic] final solution,"
25 Murphy explains that his final solution was randomizing

1 the output within a certain range using a Gaussian
2 function, correct?

3 A. Yes.

4 Q. How does the -- can you explain how the
5 Gaussian function is used to randomize and thereby
6 obfuscate the results?

7 A. I cannot.

8 Q. Do you have an understanding of what Murphy is
9 likely referring to here?

10 A. Yeah. I mean, they're attempting to
11 randomize, and there are a number of ways -- evidently,
12 using a Gaussian function is one -- to randomize the
13 output so that you are forced towards a mean, according
14 to them.

15 But this is one final solution. That's not
16 necessarily required.

17 Q. And, again, why is Murphy trying to randomize
18 the output?

19 A. It's seeking to prevent inference of the PII.
20 So one of the solutions is to not return less than three
21 results, and the other one that they offer up is to
22 randomize the output.

23 Q. So the obfuscated result then obfuscates the
24 true number of patients in the group that are identified
25 in response to the query?

1 A. I mean, that's one possibility.

2 Q. Okay. Then the -- and the right-hand side of
3 page 555, about a third of the way down, Murphy says,
4 (as read) "We modify our range algorithm to have a wider
5 obfuscation at values close to zero and indicate the
6 greater range by returning '<3' when the obfuscated
7 number is less than three."

8 Is that right?

9 A. That's what it says.

10 Q. So if Murphy -- is it your understanding that
11 Murphy produces the obfuscated number when the
12 obfuscated number is not less than three?

13 A. I think it allows for that possibility. But
14 here specifically, it says, (as read) "When the
15 obfuscated number is less than three," is what the
16 sentence says.

17 Q. Right. So when the obfuscated number is less
18 than three, then it returns an indication of the range
19 as less than three, right?

20 A. That's what it says.

21 Q. But when the obfuscated number is not less
22 than three, then it produces a result that it's just the
23 obfuscated number itself; is that right?

24 A. That's one possibility. I mean, it can --
25 basically the limitation that we were seeking to find

1 was an explicit disclosure in the field of limiting the
2 number of records returned, and this provides it.

3 Q. So Murphy -- but it returns a response to the
4 query regardless of whether the obfuscated number is
5 less than three, equal to, or greater than three; is
6 that correct?

7 A. No. That's not the way I understand that.

8 I understand that, if it's less than three, it
9 tells you it's less than three. So it's limiting the
10 number.

11 Q. And when the number is greater than three, a
12 possibility is for Murphy to provide the number, the
13 obfuscated number, correct?

14 A. That's one of the possibilities that it
15 discloses, yes.

16 Q. Okay. Let's turn to the Dick reference,
17 Exhibit 1007.

18 A. All right.

19 Q. I'm going to ask the same questions I've asked
20 with respect to Evenhaim and Murphy.

21 So did you review Dick while preparing your
22 declaration in this proceeding?

23 A. Yes.

24 Q. Have you read Dick in its entirety?

25 A. Yes.

1 Q. How did you first encounter the Dick
2 reference?

3 A. This one was provided by the attorneys as
4 well.

5 Q. To your recollection, were you aware of Dick
6 before your involvement in the present proceeding?

7 A. I don't think so.

8 Q. And do you believe that you have a good
9 understanding of the technology described in Dick?

10 A. Yes.

11 Q. I'd like to turn to Figure 3, please, of Dick.

12 A. Okay.

13 Q. And Figure 3 generally describes the system
14 for requesting and retrieving medical information,
15 correct?

16 A. Yes.

17 Q. Dick's system can process requests for
18 de-identified medical information and can return such
19 information in response to requests, correct?

20 A. That's one of the things it describes, yes.

21 Q. And in Figure 3, there are multiple components
22 to a system, correct?

23 A. Yes. Different -- it discloses sort of a
24 high-level architecture and functions.

25 Q. One of those components is a requesting and

1 viewing client, correct?

2 A. Yes.

3 Q. There are three different options disclosed.
4 A first option, client/server; a second option, intranet
5 based; and a third option, internet based; is that
6 correct?

7 A. Those are the ones that are shown. There
8 could be others.

9 Q. What is the function of the requesting and
10 viewing client in Dick?

11 A. It's submitting queries.

12 Q. So, for example, the requesting and viewing
13 client, 215, would submit a request to the requester's
14 server; is that correct?

15 A. It would be routed through the requester's
16 server, but, yes.

17 Q. And the request would be routed through the
18 requester's server to the Central Server?

19 A. That's correct.

20 Q. What is the function of the requester's
21 server, 230, in Dick?

22 A. It routes the request to the Central Server.

23 Q. Are there any other functions disclosed for
24 the requester's server in Dick?

25 A. I don't know. I don't have total

1 recollection. I can search it once again, if that's
2 where you want to go.

3 Q. Sitting here right now, you don't recall any
4 other functions?

5 A. No, I don't have total recall of the
6 reference.

7 Q. And the system further includes a Central
8 Server, 245, correct?

9 A. Yes, as we discussed.

10 Q. There are four dashed boxes showing the
11 Central Server that describe different functions of the
12 server.

13 Do you see that?

14 A. Yes.

15 Q. And so the Central Server is responsible for
16 formatting a query based on requests received from the
17 requesting and viewing client; is that correct?

18 A. That's one of the things it can do, yes.

19 Q. Is there a difference between a request and a
20 query in Dick?

21 A. I think so. I think the query is formatted
22 according to the protocol. The request is probably a
23 higher-level request.

24 Q. And how would the query be formatted according
25 to the protocol?

1 A. Well, it would depend upon the back-end
2 databases. It would be similar to the aggregator that
3 we discussed at some length in Evenhaim where you have
4 the Central Server that has to create a meaningful query
5 that the -- will produce results from the databases it's
6 talking to.

7 Q. And so the Central Server would format a query
8 based on a receipt for request and forward the query to
9 the archived medical information system or the medical
10 information repository; is that correct?

11 A. Yeah. Those are the back-end data sources.

12 Q. Do you understand that Dick uses the shorthand
13 AMIS, or A-M-I-S, for archived medical information
14 system?

15 A. I've seen that, yes.

16 Q. Okay. And then similarly, MIR for the medical
17 information repository?

18 A. Yes, I've seen that too.

19 Q. Dick, at paragraph 28, gives some examples of
20 the medical information repository.

21 Let me know when you see that.

22 A. I'll scroll.

23 Q. Sure.

24 A. All right. Give me a moment.

25 Okay.

1 Q. And so some of those examples include a
2 pharmacy benefit manager, a pharmacy -- physician's
3 office, or clinical laboratory that stores identified
4 patient information; is that correct?

5 A. Yes. Physician's office is also listed.

6 Q. The medical information repository would then
7 be a covered entity under HIPAA?

8 A. If it has PII, it is for sure.

9 Q. Same as the archived medical information
10 system?

11 A. If it has PII in it, then it's covered.

12 Q. And what's the difference between the archived
13 medical information system and the medical information
14 repository intake?

15 A. The difference listed is that the AMIS server
16 can archive for longer periods of time than the MIR, but
17 there may be other differences.

18 Q. The query that's transmitted from the Central
19 Server could be queried to either the archived medical
20 information system or the medical information
21 repository?

22 A. I mean, according to the diagram, it looks
23 like it could be passed through, yeah.

24 Q. The Central Server, as we mentioned earlier,
25 receives the request and then formats the request for

1 the query, right?

2 A. That's the way I would expect it to work, yes.

3 Q. Are there any other components of the system
4 that format the request for the query?

5 A. I mean, it's certainly allowed by the
6 reference.

7 Q. But it -- are you aware of any disclosure in
8 Dick of anything except for the Central Server
9 formatting a request for the query?

10 A. Well, the database is, again, on the back side
11 for the AMIS and the MIR. They are going to do some
12 sort of formatting depending upon what type of DBMS and
13 searching that they are doing.

14 So, yeah, I would expect some processing to
15 occur on those systems.

16 Q. Some processing to occur at which system?

17 A. AMIS and MIR, depending upon where the query
18 goes.

19 Q. The requester's server is never disclosed in
20 Dick as formatting a query for the AMIS or the MIR,
21 correct?

22 A. I don't remember an explicit disclosure on
23 that. It is certainly possible. I wouldn't expect it
24 to work that way.

25 Q. So after the Central Server sends a query to

1 AMIS or MIR, AMIS or MIR will return a result to the
2 Central Server; is that correct?

3 A. Well, that's where they have the data. So
4 they are going to have to provide that data in response
5 to the query.

6 Q. And they provide the data back to the Central
7 Server?

8 A. Yes.

9 Q. And the response that AMIS or MIR provide to
10 the Central Server, is the medical information
11 de-identified?

12 A. That's certainly possible.

13 Q. And I'll -- I guess I'll clarify.

14 Would it be de-identified when the patient has
15 not provided authorization for the release of PII?

16 A. That would be a reasonable way to do it, yes.

17 Q. And is that what Dick discloses happens?

18 A. That's one of the possibilities, yes.

19 Q. Is there a difference between a possibility
20 and what Dick discloses?

21 A. Yeah. I mean, again, it's disclosing an
22 architecture for a system. And as we've discussed a
23 fair amount, I mean, it's possible to move functions
24 across servers when you're -- when we actually go to
25 implement one of these systems.

1 Q. As Dick describes the embodiment that's shown
2 in Figure 3, do the AMIS and MIR --

3 (Court reporter requested clarification.)

4 BY MR. STEPHENS:

5 Q. Does Dick describe in the embodiment of
6 Figure 3 that AMIS or MIR returns de-identified patient
7 data to the Central Server?

8 A. I'm looking.

9 Well, the description in Figure 3 says it --
10 Figure 3 illustrates several preferred physical
11 environments in which the method of the preferred
12 embodiment may be carried out. So by definition, we
13 know that we can move those functions around is what
14 that disclosure is telling us.

15 Let me see if I can find something even more
16 explicit for you.

17 Yeah, it says at 24 that the identification
18 could be done by patient number, which would be
19 de-identified. So it certainly allows for that
20 possibility.

21 Q. Does paragraph 45 also support that the
22 medical information repository would return
23 de-identified data?

24 A. Let's see what 45 says.

25 Well, that -- 45 is referring before it can be

1 released back to the requesting client. So it looks to
2 me like it could be either/or as far as the AMIS and MIR
3 are concerned.

4 Q. And how is the response to the query routed
5 back to the client in Figure 3?

6 A. I understand it to be going through the
7 Central Server to the requester's server.

8 Q. And the requester's server then forwards it to
9 the requesting client?

10 A. Yes, unless -- I mean, you can also look that
11 the intranet and internet connections go through the
12 firewall to that server. So, I mean, there's some
13 ambiguity there. But if I were implementing the system,
14 they would all work the same way.

15 Q. And then the patient data would be -- would be
16 de-identified when it reaches the requester's server,
17 correct?

18 A. Unless there's a signed authorization form
19 with it.

20 Q. Right.

21 Would a POSITA understand the requesting and
22 viewing client is a noncovered entity?

23 A. I mean, that's one possibility. I wouldn't
24 say it has to be that way.

25 But, I mean, it -- it would be possible to

1 implement this system in such a way that the requesting
2 client wasn't covered.

3 Q. And similarly, it would be -- would it be
4 possible to implement the system in a way that the
5 requester's server is not a covered entity?

6 A. Yes. For the same reasons.

7 Q. And likewise, would it be possible to
8 implement the system where the Central Server, 245, is
9 not a covered entity?

10 A. I mean, anything is possible. That's going to
11 be harder. Like I said, this -- the Central Server is
12 like the aggregator of Evenhaim.

13 So, in general, it has to be trusted, but it
14 would be possible -- I mean, you could implement and
15 architect the system in such a way that it never
16 processed PII.

17 Q. Does Dick disclose any methods for
18 de-identifying patient data?

19 A. I'm going to have to search the whole
20 document. I don't have recollection of specific
21 methods.

22 I mean, a person of skill certainly would know
23 what cryptographic methods were available. But let me
24 search.

25 Q. Yeah. I think I'll -- I'm thinking of

1 paragraph 45 as one example.

2 A. All right. Let's have a little reading.

3 Well, 45 says "de-identifying methodology,"
4 which is what I said. I mean, any number of way
5 cryptographic mechanisms are known to do that.

6 46 says --

7 Well, I'm not finding a reference to hash or
8 encryption. So it -- it may be that it assumes the
9 knowledge of the reader as to what -- to know what
10 de-identifying methodologies are.

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

13 A. Should.

14 Q. And could those methodologies include things
15 other than encryption and crypto -- I'm sorry,
16 cryptographic techniques?

17 A. I mean, it's certainly possible that you could
18 use other types of IDs or pseudonyms for PII, but
19 generally speaking, I think they would use cryptographic
20 mechanisms.

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.

1 And, I mean, any number of libraries that are out on the
2 Internet to do that.

3 Q. All right. Could we turn to the Landi
4 reference, Exhibit 1008.

5 A. All right. Got it.

6 Q. You're familiar with the Landi reference,
7 correct?

8 A. Yes.

9 Q. Did you review Landi in the course of
10 preparing your declaration?

11 A. Yes.

12 Q. And have you read Landi in its entirety?

13 A. Yes.

14 Q. How did you first encounter the Landi
15 reference?

16 A. This is another one provided by the attorneys.

17 Q. To your recollection, were you familiar with
18 Landi before your involvement with this IPR?

19 A. I don't think so.

20 Q. And do you believe you have a good
21 understanding of the technology described in Landi?

22 A. Yes.

23 Q. At Column 1 of Landi, around line 12, there's
24 a section that's titled "Technical Field of the
25 Invention."

1 Do you see that?

2 A. Yep.

3 Q. And this section describes what the present
4 invention relates to, correct?

5 A. I mean, it's -- the field of the invention is
6 the protection of privacy of healthcare data is what it
7 says.

8 Q. Starting at line 16, it says, "In
9 particular" -- it's carrying over from the present
10 invention -- "in particular, to systems and methods that
11 implement secured key encryption for de-identifying
12 patient data to ensure patient privacy while allowing
13 only the owners of the patient data records and/or other
14 legally empowered entities to reidentify subject
15 patients of de-identified data records when needed."

16 Do you see that?

17 A. That's what it says.

18 Q. Why would the owners of the patient data
19 records or other legally empowered entities need to
20 reidentify the patients?

21 A. Any number of reasons. I mean, if you had a
22 data coherency problem, you might want to undo the
23 de-identification so that you could fix the coherency of
24 the database, for instance. It also --

25 Q. All right.

1 Oh, go ahead.

2 A. -- looks like there's -- looks like there's
3 law, legally empowered entities, I would assume maybe to
4 be law enforcement or something like that or Court
5 order.

6 So those -- those would be entities that might
7 have a need to reidentify the data.

8 Q. Would you agree that a central focus of Landi
9 was allowing for reidentification of patients?

10 A. No. I think that that's a feature of using
11 reversible encryption, but I don't think that was the
12 focus. The focus is protecting patient privacy.

13 Q. And Landi identified reidentification as an
14 aspect of his invention, correct?

15 A. Right. If you use reversible encryption, then
16 reidentification is possible if you get access to the
17 keys.

18 Q. So reidentification would be possible if you
19 had the patient's de-identified data record, the
20 encrypted ID, and a decryption key?

21 A. And the algorithm for the --

22 (Court reporter requested clarification.)

23 THE WITNESS: The algorithm for the encrypted
24 data.

25 BY MR. STEPHENS:

1 Q. All right. Let's turn to Figure 1, please.

2 Are you there?

3 A. Almost.

4 Q. Sure.

5 A. Okay.

6 Q. And so Figure 1 provides an overview of the
7 system disclosed in Landi, correct?

8 A. Yeah. It's a high-level architecture diagram,
9 if you will.

10 Q. And that diagram shows a set of patient data
11 processing systems, 20-1 through 20-n, correct?

12 A. Yes.

13 Q. The system further includes a central patient
14 data processing system, 30; is that correct?

15 A. Yes.

16 Q. And then a central surveillance system, 50,
17 correct?

18 A. Yes.

19 Q. And the patient data processing systems, 20,
20 are operated at different clinical sites by different
21 healthcare organizations, correct?

22 A. For this embodiment, yes.

23 Q. The patient data processing systems maintain
24 identified patient data, correct?

25 A. That's what's shown in this particular figure,

1 yes.

2 Q. And the identified patient data is indicated
3 by 21; is that correct?

4 A. I don't understand your question.

5 Q. Yeah. I'm sorry.

6 Within patient data processing systems, 20,
7 there's a cylinder labeled "21" that's -- or numbered 21
8 that's labeled "Identified Patient Data."

9 Do you see that?

10 A. I do.

11 Q. And so what would be contained in the
12 identified patient data repository?

13 A. I understand that to be data that needs to be
14 protected. So it would have PII in it.

15 Q. So the patient data processing systems are
16 analogous to the medical information repository in Dick,
17 in that they both maintain identified patient data?

18 A. Yeah. They could actually be both -- since
19 the MIR and the AMIS are passing information back and
20 forth, this could fulfill actually both functions.

21 Q. I'm sorry. What do you mean by "both
22 functions"?

23 A. You were asking me how this maps to Dick, and
24 I'm saying this is -- the servers that contain the PII
25 in Dick would be represented here.

1 Q. Right. Like the medical information
2 repository in Dick?

3 A. Or like the AMIS in Dick, yes.

4 Q. Yes.

5 And Landi discloses that the patient data
6 processing systems can produce de-identified patient
7 data using an encryption system; is that correct?

8 A. That's the intent of this embodiment, yes.

9 Q. How does the encryption system work in Landi?

10 A. It has -- it's a public key-based,
11 key-management system.

12 Q. And so how does the encryption system generate
13 an encrypted ID for the patient data processing systems?

14 A. It would encrypt with a public key at some
15 level.

16 Q. That encrypts PII with the public key?

17 A. That's one way to do it. It can also
18 encrypt -- you've also got a key generation engine down
19 there, so it could be that you were generating symmetric
20 keys that were used to encrypt the data that were then
21 encrypted with the public key.

22 But essentially the public key -- or the
23 private key would control access to that data after it's
24 encrypted.

25 Q. And the encryption systems are located in the

1 patient data processing systems in Landi; is that
2 correct?

3 A. That's where the actual encryption occurs,
4 yes.

5 Q. There's no other use of the encryption systems
6 outside of the patient data processing systems, correct?

7 A. For this embodiment, the encryption is
8 controlled within those systems so that the -- what is
9 released is de-identified patient data.

10 Q. And the de-identified patient data is then
11 released to the central patient data processing system?

12 A. Right. That's the -- that's where the queries
13 would be matched.

14 Q. And the central surveillance system, 50,
15 includes a master private key.

16 Do you see that?

17 A. I do.

18 Q. What would the master private key be used for?

19 A. As I said, depending on how it's implemented,
20 it would probably be used to access individual symmetric
21 keys that were used to do the encryption, but it could
22 also be used to access and reidentify patient data is
23 essentially what its use is.

24 Q. The patient data processing systems -- going
25 back to the top of the figure -- those would be covered

1 entities under HIPAA, correct?

2 A. If they have PII, they are covered.

3 Q. And then the central patient data processing
4 system, 30, would not be a covered entity under HIPAA;
5 is that correct?

6 A. It may, or it may not be. Again, to the
7 extent it has access to PII because it's talking with
8 the server that has the master private key, then it
9 would be covered. But, I mean, there are a variety of
10 ways to implement this architecture.

11 Q. As shown in Figure 1, there is no identified
12 patient data repository within the central patient data
13 processing system, correct?

14 A. That doesn't mean that it doesn't have access
15 to the PII.

16 Q. But it's not shown in Figure 1?

17 A. It is shown, to somebody who understands the
18 key management and cryptography, that it's possible for
19 30 to have access to PII by virtue of the data flows
20 that exist.

21 Q. Again, is there any disclosure in -- in Landi
22 that -- in which the central patient data processing
23 system has identified patient data?

24 A. Yes, as I've just described to you.

25 Q. So you are inferring that from the

1 communications?

2 A. I'm not inferring anything. As a person well
3 versed in cryptography, I'm telling you that it's
4 possible, depending upon those data flows, for the
5 server, 30, to have access to PII, which would make it
6 covered.

7 Q. Would you agree that just because something is
8 possible does not mean that it is disclosed in the
9 reference?

10 A. No. I mean, if one of skill in the art would
11 understand that disclosure, then it's disclosed.

12 Q. You're unable to point to any text in Landi in
13 which the central patient data processing system
14 includes identified patient data?

15 A. False. I just explained how it could have
16 access to the PII.

17 Q. But you're not aware of any text that
18 discloses identified patient data within the central
19 patient data processing system?

20 A. I don't know if it goes through and explains
21 it. I'm telling you what I'm looking at and what a
22 person of skill would understand or a person who at
23 least understands cryptography would understand this to
24 disclose.

25 MR. STEPHENS: All right. It's 1:00 p.m.

1 Eastern right now.

2 Should we take a -- I think this would be a
3 good time for a lunch break, if that's okay with you,
4 Dr. Clark.

5 THE WITNESS: Depends on how much longer you
6 want to go with this. If you think we're going to go a
7 few more hours, then probably. If you're going to try
8 and wrap up in another hour or so, then I'm happy to
9 work with you and power through. It's up to you.

10 MR. STEPHENS: Why don't we take 30 minutes
11 and reconvene at 1:30.

12 THE WITNESS: Okay.

13 MR. STEPHENS: Okay.

14 (Recess: 1:01 p.m. to 1:38 p.m. EST.)

15 BY MR. STEPHENS:

16 Q. All right. Welcome come back from lunch,
17 Dr. Clark.

18 During the break, did you have any discussions
19 about the substance of your testimony with anyone?

20 A. Nope.

21 Q. Let's turn to paragraph 214 of your
22 declaration.

23 A. Okay.

24 Q. Okay. And this paragraph is in the context of
25 your analysis of the Dick and Landi combination,

1 correct?

2 A. Yes.

3 Q. I have a few questions for you just to help
4 clarify your understanding of what this combination is.

5 So as described at paragraph 214, we
6 understand that, in this combination, you're proposing
7 to implement Landi's encryption server and Dick's
8 requester's server; is that correct?

9 MR. OLIVER: Objection. Foundation.

10 THE WITNESS: So can you re-ask your question?
11 It was a little unclear to me.

12 BY MR. STEPHENS:

13 Q. What are you proposing to modify in Dick to
14 integrate a requester's server -- I'm sorry, integrate
15 an encryption server?

16 A. If we look at Figure 3, I mean, it's basically
17 what you need is the token or de-identified database
18 that Landi discloses and plug it into Dick, so there's
19 multiple ways one might do that.

20 One is at the Central Server. You could also
21 replace the requester's server, insofar as it's only
22 routing information to. So the main idea is that you're
23 replacing the PII-containing databases with those of
24 Landi and then the token -- also the token system of
25 Landi and plugging it into Dick.

1 And there's more than one way to do that,
2 obviously.

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.

22 Q. And as a further modification of Dick's
23 system, are you proposing that Landi's central patient
24 data processing system could be queried in lieu of the
25 AMIS or MIR?

1 A. Yes, absolutely, because the PII of Landi --
2 of Landi comes from those data sources, so the query
3 would be routed to them. As I said, much the same as
4 what we described in Evenhaim.

5 Q. And so the query -- would the query and the
6 response follow a similar path as Dick describes through
7 the requester's server -- Central Server and then to the
8 central patient data processing system in your
9 combination?

10 MR. OLIVER: Objection. Form.

11 THE WITNESS: Yeah. What -- the requesting
12 client -- and you have three types -- would make a
13 request through that would be routed to the system of
14 Landi to satisfy it with de-identified information.

15 BY MR. STEPHENS:

16 Q. In the proposed combination, the response
17 would be routed back to the requesting client through
18 the requester's server; is that right?

19 A. Yes. So basically the data flows would be the
20 same. It's just that you would have to have the
21 de-identified information produced and then delivered to
22 the client.

23 Q. And so that de-identified information in Landi
24 is -- includes the encrypted ID, correct?

25 A. It could.

1 Q. In the combination, the encrypted ID would be
2 routed to the requesting client through the requester's
3 server?

4 A. That's possible, sure.

5 Q. That's consistent with your description of the
6 combination?

7 A. I think so.

8 Q. Okay. Let's turn to the Settimi reference,
9 Exhibit 1006.

10 A. Okay.

11 Q. And you're familiar with Settimi, correct?

12 A. Yes.

13 Q. Have you reviewed it in its entirety?

14 A. Yes.

15 Q. Were you aware, to your knowledge, of the
16 Settimi reference before your work on this IPR?

17 A. I may have been, but it -- it was provided by
18 the attorneys, in answer to your next question.

19 Q. All right. Let's take a look at Figure 2 of
20 Settimi, please.

21 A. Okay.

22 Q. Can you describe what's shown in Figure 2?

23 A. It's the data architecture for that
24 embodiment.

25 Q. There's a collection of PCPs shown in

1 Figure 2, correct?

2 A. PCPs, you mean?

3 Q. Yes.

4 A. Yes.

5 Q. The PCPs are patient care providers, correct?

6 A. Yes.

7 Q. And the PCPs communicate with the data
8 warehouse system?

9 A. Yes.

10 Q. Which produces a patient cohort report, 212?

11 A. Yes.

12 Q. And then each of the PCP maintains an
13 electronic medical records database, correct?

14 A. Yes.

15 Q. The PCPs release de-identified patient data to
16 the data warehouse; is that correct?

17 A. In this embodiment, yes.

18 Q. Are there other embodiments of which you're
19 aware in which the patient data is not de-identified
20 before release to the data warehouse system?

21 A. I'd have to review the entire reference. I
22 mean, that's the interesting one.

23 Q. But sitting here now, you don't recall such
24 embodiments?

25 A. I don't have total recall of the reference,

1 no.

2 Q. The data warehouse system includes a data
3 import function, 206.

4 Do you see that?

5 A. I do.

6 Q. And what does the data import function do?

7 A. It does the aggregation and deidentification
8 of the patient data from the sites.

9 Q. Is that from paragraph 35?

10 A. That's from paragraph 35.

11 Q. Would aggregating patient data include merging
12 patient data records?

13 A. It could include lots of things. I mean, data
14 aggregation. I mean, they might change the structure.
15 They do all sorts of processing on the data.

16 Q. Could you elaborate? What would aggregating
17 data in this context mean to you?

18 A. I would think it would include linking things
19 like canonicalization, other things that would make the
20 system function better.

21 (Court reporter requested clarification.)

22 BY MR. STEPHENS:

23 Q. And in your declaration, you analyzed Settimi
24 in the context of a combination with Evenhaim, correct?

25 A. Yes.

1 Q. Your declaration did not rely on Settimi as
2 disclosing the encryption server; is that correct?

3 A. No. It was a combination to allow Evenhaim to
4 query de-identified information.

5 Q. So the mapping through the encryption server
6 in the Evenhaim/Settimi combination would be the same as
7 your mapping in the Evenhaim first draft one.

8 A. Yes.

9 MR. STEPHENS: All right. I think we're near
10 the end here.

11 Could we take ten minutes? I'll confer with
12 our team and see if we have further questions.

13 THE WITNESS: Absolutely.

14 MR. STEPHENS: All right. Why don't we return
15 at 2:05.

16 (Recess: 1:55 p.m. to 2:06 p.m. EST).

17 BY MR. STEPHENS:

18 Q. All right. Welcome back, Dr. Clark.

19 During the break, did you discuss the
20 substance of your testimony with anyone?

21 A. Didn't discuss anything with anybody.

22 MR. STEPHENS: We have no further questions.
23 We pass the witness.

24 MR. OLIVER: Thank you.

25 I have no questions for the witness.

THE SULLIVAN GROUP OF COURT REPORTERS

1 COURT REPORTER: Counsel, may I get transcript
2 requests on the record.

3 MR. STEPHENS: Yeah. I think that, our order,
4 we had asked for a rough in 48 hours and then final by
5 October 3rd. Could we get the rough within 24.

6 COURT REPORTER: Yes.

7 MR. STEPHENS: And then final is still okay
8 for October 3rd.

9 COURT REPORTER: Perfect.

10 MR. OLIVER: And I don't need a copy. There
11 will be a copy made public in the file, so I'm good for
12 right now. But thank you.

13 (Whereupon the proceedings concluded at
14 2:08 p.m. EST)

15

16

17

18

19

20

21

22

23

24

25

THE SULLIVAN GROUP OF COURT REPORTERS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

ERRATA SHEET

NAME OF CASE: DATAVANT, INC. V. VIGILYTICS LLC
DATE OF DEPOSITION: September 26, 2024
NAME OF WITNESS: DR. PAUL CLARK

Reason Codes:

- 1: To clarify the record.
- 2: To conform to the facts.
- 3: To correct transcription error.

Page	_____	Line	_____	Reason	_____
From	_____				to _____
Page	_____	Line	_____	Reason	_____
From	_____				to _____
Page	_____	Line	_____	Reason	_____
From	_____				to _____
Page	_____	Line	_____	Reason	_____
From	_____				to _____
Page	_____	Line	_____	Reason	_____
From	_____				to _____
Page	_____	Line	_____	Reason	_____
From	_____				to _____
Page	_____	Line	_____	Reason	_____
From	_____				to _____

_____	_____
DR. PAUL CLARK	DATED

DECLARATION UNDER PENALTY OF PERJURY

I, DR. PAUL CLARK, do hereby certify under penalty of perjury that I have read the foregoing transcript of my deposition taken on September 26, 2024; that I have made such corrections as appear noted on the Deposition Errata Page(s), attached hereto, signed by me; that my testimony as contained herein, as corrected, is true and correct.

This Declaration is executed this _____ day of _____, 20____, at _____, California.

DR. PAUL CLARK

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25

**I, Tamara Houston, RPR, CCRR, CSR No. 7244, a
Certified Shorthand Reporter in the State of California,
duly empowered to administer oaths, do hereby certify:**

That said deposition was taken down by me in shorthand at the time and place therein named, and thereafter reduced to typewriting by computer-aided transcription under my direction;

I further certify that I am not interested in the event of the action.

Dated: 3rd of October, 2024.

TAMARA L. HOUSTON
CSR 7244, RPR, CCRR 140

THE SULLIVAN GROUP OF COURT REPORTERS

-	1999 16:22 17:25	245 72:8 79:8	45 77:21,24,25 80:1,3
--o0o-- 6:2	1:00 89:25	25 15:1,5,6	46 80:6
1	1:01 90:14	26 6:1 21:14,17 48:10	48 98:4
1 25:7 35:24 81:23 84:1,6 88:11,16	1:30 90:11	28 22:2 24:22 73:19	4A 27:24 28:8,13
1001 9:2 25:8	1:38 90:14	2:05 97:15	4B 28:13
1003 9:21 13:18	1:55 97:16	2:06 97:16	5
1004 16:13	2	2:08 98:14	5 32:2,5 44:11,18 45:3
1005 10:2 26:23	2 15:15 94:19,22 95:1	3	50 84:16 87:14
1006 10:6 94:9	20 11:3 56:20 84:19 85:6	3 31:9 40:7 42:12,16 43:24 68:6 70:11,13,21 77:2,6,9,10 78:5 91:16	55 66:23
1007 10:10 69:17	20-1 84:11	30 25:11 84:14 88:4,19 89:5 90:10	555 65:17,22 66:4 68:3
1008 81:4	20-n 84:11	33 37:8	590 15:17
1009 10:16 64:14	2000s 38:17	35 96:9,10	6
10:50 45:20	2009 21:25	36 37:8	641 8:25 14:8 22:5 23:10, 14,24 24:8,17,25 25:7 61:7
11:04 45:20	2024 6:1	39 55:12	7
11:47 64:11	2024-00226 6:24 9:8	3rd 98:5,8	7 13:17 35:24 41:23 55:12
12 45:25 46:7 47:20 48:10 81:23	206 96:3	4	8
12:06 64:11	21 85:3,7	4 27:23,24 28:3,16 29:15 30:7 35:22 36:6,16 37:6 40:7 41:22 42:9,12 43:1,24 56:22 58:23 59:3 60:3	86 62:9
13 37:8 40:13 42:24 46:16	212 95:10	40 56:17,21	9
14 40:7 41:22	214 90:21 91:5 92:3	42 61:1,18 62:1	9118641 6:24 9:3
16 47:20 82:8	215 71:13		9:38 6:1
1995 15:1 17:25	230 71:21		
	24 77:17 98:5		

THE SULLIVAN GROUP OF COURT REPORTERS

A A-M-I-S 73:13 a.m. 6:1 45:20 64:11 abovementioned 40:8 absence 62:15 absolutely 93:1 97:13 abstract 34:19 access 18:21 20:16 30:6,19,21, 24 31:2,3,5,12 34:22 35:21 36:8 48:25 49:7 50:3 52:14 83:16 86:23 87:20,22 88:7,14,19 89:5,16 accessing 31:22 accordance 21:23 accurate 8:13 acknowledges 56:5 acronym 9:11 ACSAC 20:9 actual 87:3 add 25:3 added 61:7 addition 40:4 additional 26:13 61:6,10,17 62:4 address 17:15	adopted 22:3,24 23:18 24:4,15 advised 41:23 aggregates 36:12 aggregating 96:11,16 aggregation 96:7,14 aggregator 28:10 30:8,11,15,24 31:5,25 32:9,17,20,22, 24 33:5,9,11,18,21 34:6,8,12,16,17,20,24 35:1,10 36:17 46:25 47:8,14,17 48:17 49:1, 14,17 50:9,19,22 51:5, 19 52:1,5,11,19,20 53:9,14,19,22 54:2 56:24 58:1,8 62:7 63:6 73:2 79:12 agree 22:12,18 29:14 42:15 44:18 58:1 83:8 89:7 agreement 22:16 ahead 51:1 64:18 83:1 AI 17:18 AI-GUIDED 17:14 aim 7:5,11 algorithm 39:12,16 68:4 83:21,23 algorithms 38:24 alleged 9:13 55:25 allowed 57:7 58:20 75:5 allowing 82:12 83:9 ambiguity	78:13 AMIS 73:13 74:15 75:11,17, 20 76:1,9 77:2,6 78:2 85:19 86:3 92:25 amount 76:23 analogous 85:16 analyses 22:15 analysis 23:16 36:14 90:25 Analyze 32:3 analyzed 96:23 and/or 48:12 82:13 answering 7:6 59:21 appearance 6:18 applied 21:22 38:21 apply 22:14,19,21 23:8 40:1 41:3 42:3 approximately 11:1 12:24 13:8 14:23 15:7,12 architect 79:15 architected 30:20 32:12 49:2 architecture 32:25 70:24 76:22 84:8 88:10 94:23 archive 74:16 archived 73:9,13 74:9,12,19 arguably 49:21	art 9:12 31:20 38:3 40:25 43:1,16 54:10,15 56:1 89:10 aspect 83:14 aspects 19:16 40:8 assistant 13:15 assume 24:20 83:3 assumes 40:16 80:8 attain 25:21 attempting 30:1 36:8 67:10 attended 65:10 attorney 6:11 11:25 attorneys 22:15 25:6 65:5 70:3 81:16 94:18 authentication 38:13 author 20:3 authorization 20:17 29:12 76:15 78:18 avoid 63:3 aware 14:10,15,16,18,19 27:11 30:23 31:4 49:25 56:10 57:4,17 62:3 65:7 70:5 75:7 89:17 94:15 95:19 B back 15:1 34:18 35:22 36:14 37:4 42:9 53:21 60:25 75:10 76:6 78:1,5 85:19
--	---	--	---

THE SULLIVAN GROUP OF COURT REPORTERS

87:25 90:16 93:17 97:18	box 32:5 44:14	47:21 95:5	cipher 39:16
back-end 73:1,11	boxes 72:10	career 14:23 19:3	circuit 46:11 47:2
background 14:1	breach 47:24 48:4,7	careful 46:8	citations 56:10 61:25
Barclay 6:15	break 7:10,11,12 45:14,22 64:5 90:3,18 97:19	carried 77:12	city 8:8
based 22:11 24:8 71:5 72:16 73:8	breaks 7:14	carry 42:1	claim 21:20 22:4 25:7,13 65:15
basically 17:1 68:25 91:16 93:19	briefly 39:13	carrying 82:9	clarification 16:1 25:4 40:17 77:3 83:22 96:21
basis 33:3 62:20	broad 26:18 44:25	case 15:2,19,23,24 33:11 34:24 49:16 55:3,5 57:2 58:25	clarify 63:16 76:13 91:4
begin 13:8	broader 24:1	cases 53:20	clarity 8:15
beginning 66:24	brought 16:16	caught 14:22	Clark 6:3,9,25 8:7 16:18 34:10 45:22 90:4,17 97:18
begins 46:3	brute 26:22	center 30:8	class 46:4
behalf 6:13,20	built 61:24	central 71:18,22 72:7,11,15 73:4,7 74:18,24 75:8,25 76:2,6,10 77:7 78:7 79:8,11 83:8 84:13,16 87:11,14 88:3,12,22 89:13,18 91:20 92:8,10, 17,23 93:7,8	clean 7:5
benefit 28:5 74:2	bullet 24:21		Clear 17:8,12,22
Bethesda 8:9	bunch 14:2		client 18:20 19:4,10,13 71:1, 10,13 72:17 78:1,5,9,22 79:2 93:12,17,22 94:2
big 21:8		CEO 17:8,14	client/server 71:4
biggest 21:7	call 50:11 53:17	change 96:14	clinical 74:3 84:20
binder 7:19	called 6:4 43:18	changed 14:13	clinician 17:20
bit 17:17 45:12,16	canonicalization 96:19	channel 40:22 41:16	close 68:5
bits 39:15	capabilities 30:14	characterizes 22:9 24:15	co-authors 20:6
books 38:14	capability 50:14,19	chief 18:1,5	codes 38:13
bottom 56:20	capable 47:22 52:9	choose 41:6	coherency
boundary 36:25 37:1,3 47:6 48:21,23,24 49:6,18	capacity 11:13 12:1	Christopher 8:7	
	care		

THE SULLIVAN GROUP OF COURT REPORTERS

82:22,23	compliant 19:18 92:16,21	consultant 52:25	69:6,13 70:15,19,22
cohort 95:10	comply 21:2 49:3 56:23 62:17	consulting 11:16 15:17	71:1,6,14,19 72:8,17
collaborated 11:19	complying 29:6	consumer 28:9 29:16,24 30:3	73:10 74:4 75:21 76:2
collaborative 12:12,15,21	components 70:21,25 75:3	consumers 28:19,21 29:23	78:17 81:7 82:4 83:14
colleagues 6:14	compromising 46:12	contained 14:8 60:8 85:11	84:7,11,14,17,21,24
collection 94:25	computationally 25:21,22 26:9,11,22	contents 12:22 41:18	85:3 86:7 87:2,6 88:1,5,
column 37:8 40:7,13 41:22	computer 17:20 23:19,21 25:24	context 90:24 96:17,24	13 91:1,8 92:5 93:24
42:24 45:25 47:20	computing 28:4,9	contingent 15:23	94:11 95:1,5,13,16
48:10 55:12 66:24	concerned 19:5,11 78:3	contradict 24:1	96:24 97:2
81:23	concluded 98:13	contradicts 23:17 24:12 44:7	correctly 37:14 46:14
combination 90:25 91:4,6 93:9,16	conditions 43:19	control 20:15 86:23	correlate 47:14
94:1,6 96:24 97:3,6	confer 97:11	controlled 87:8	correlated 31:5
commercial 18:10	conference 20:2 65:10	controlling 18:21	counsel 6:17 10:21 11:23 12:20,
common 46:10,12,21 47:9	conjunction 39:1	copies 7:19,23	25 13:5,14 22:20 45:23
communicate 95:7	conjunctive 34:21	copy 16:13 98:10,11	98:1
communication 8:2 36:22 40:14	connections 78:11	correct 7:3,20 13:20 15:10,18	countermeasures 39:1
communications 89:1	considered 13:19,23	16:19,20 17:10 18:2,3	couple 15:14 27:14
companies 17:5,6,23 21:7 50:5	consistent 23:13,23 24:9,16,20	21:3,20,25 22:5,9,12	court 16:1,3,6,9 22:14 40:17
company 17:1 19:8 28:4 29:15,20	94:5	23:2,7,10,11,21 24:6,25	77:3 83:4,22 96:21
36:8 37:6 58:24 59:4	constructing 31:1	25:16 27:1 28:6,10 29:6	98:1,6,9
compared 24:5	construction 21:20 22:24 23:5,12,19,	30:4,9,16 31:11 32:6,	covered 20:19,22,24 21:4,10
compensated 15:16,20	23 24:4,9,16,23 55:24	10,22 33:5,6 34:17	29:8 30:4,16,21 36:8
compensation 15:22	constructions 22:4,12,14,18,21	35:15,24 36:18,22	48:9 50:4 51:11,19
complete 28:22 30:25 61:20		37:18 40:15 41:4 42:1,	57:6,19 59:16,19 74:7,
compliance 19:14,22		13 43:11 45:3 46:5,17	11 79:2,5,9 87:25 88:2,
		47:2,9,15,25 48:18	4,9 89:6
		49:14,18 50:7,23 51:9,	create 25:1 31:3 35:19 51:3
		12,15,20 53:4 55:18	52:15 62:25 73:4
		56:2 58:9,17 59:9,11,13	creating 55:15,20
		60:9,14,20 61:8,19 62:1	criticized 16:6
		64:19 66:1,6,11 67:2	Crossix 28:5 30:7 31:21 36:9,
			10,11 37:2 42:12 59:14
			cruncher 32:6,8,16,21 33:4,8,12,
			20 34:7 44:13
			crunching

THE SULLIVAN GROUP OF COURT REPORTERS

53:18	76:3,4,6 77:7,23 78:15	82:11	depend
crypto	79:18 80:25 82:6,12,13,	dealing	58:12 61:23 73:1
80:15	15,18,22 83:7,19,24	19:22	depending
cryptographic	84:10,14,19,23,24 85:2,	declaration	32:24 42:6 49:2 51:6
79:23 80:5,16,19	6,8,12,13,15,17 86:5,7,	9:19,20 10:23 11:6,9	75:12,17 87:19 89:4
cryptographically	13,20,23 87:1,6,9,10,	12:8,12,15,18,23,25	depends
26:21	11,22,24 88:3,12,19,22,	13:9,15,17,20 14:4,9,	26:3 30:19 32:12 35:11
cryptography	23 89:4,13,14,18,19	13,14,17,20 15:15	36:23 39:6,21,24 42:19
88:18 89:3,23	92:24 93:2,8,19 94:23	21:15,19 23:13 27:4	43:5 50:24 51:21 52:12,
CTO	95:7,15,16,19,20 96:2,	50:8 56:11,14 60:25	24 61:14 63:19 90:5
16:18	6,8,11,12,13,15,17	64:22 69:22 81:10	depicted
curriculum	database	90:22 92:11 96:23 97:1	29:15
16:14	30:12 32:12,25 35:20	declarations	deposed
customary	43:5,11,17 50:24 54:11,	12:19	15:10,13
21:23	19,20 63:20 75:10	decoupled	deposition
customers	82:24 91:17 95:13	57:10	6:12 7:2 9:17 10:20
18:10	databases	decrypt	11:2,5,10
CV	18:16 30:20 36:12 73:2,	44:15,24 48:5 63:2,13,	derive
17:10 19:24 20:9	5 91:23	15	26:10
cylinder	Datavant	decrypted	describe
85:7	6:20 8:17,18 11:13,16,	44:19	10:19 12:7,14 18:7
	20	decrypting	20:13 36:1 39:13 61:10
	Datavant's	48:6 62:16,24	72:11 77:5 92:9 94:22
	11:22	decryption	describes
	day	37:13 47:23 48:2 50:20	28:23 55:13 66:1,5
	7:13	63:4,24 83:20	70:13,20 77:1 82:3 93:6
	day-to-day	dedicated	description
	17:2	7:21,25 8:3	40:12 77:9 94:5
	days	deduce	design
	10:22	57:13	18:12,25 50:24
dashed	DBMS	deemed	designed
72:10	75:12	21:4	43:6 92:20
data	DDMS	define	desire
18:16,17 19:18 21:9	30:12	8:15	66:5
28:9,10,16,24 29:2,5,	de-identification	defines	detect
10,15,24 30:2,3,8,11,	18:17 19:17 27:14	57:11	24:6
15,24 31:5,6,11,12,16,	41:15 53:17 82:23	definition	determine
24 32:1,4,6,8,9,16,17,	de-identified	20:21 77:12	47:14 66:17
21,22 33:4,5,8,12,18,	20:18 49:13 50:1,3 52:6	degree	determining
20,21 34:12,13 35:1,6,	53:8,15 66:3 70:18	37:18 40:14	52:9
10,13,14 36:17,18,21	76:11,14 77:6,19,23	deidentification	developed
37:4,10,12,18,20,23	78:16 82:15 83:19 86:6	96:7	18:15
38:4,5,7,10,11,16,22	87:9,10 91:17 92:20	delivered	diagram
39:4,16 40:4,14,20,23	93:14,21,23 95:15,19	93:21	74:22 84:8,10
41:4,5,14,16 42:16,24	97:4	dep	Dick
43:2 44:3,13 46:5,8,10,	de-identify	7:22	10:9 69:16,21,24 70:1,
16,17,19,25 47:1,8,13	50:15,17 51:20 80:25		
48:13 49:1,12,13,16,17	de-identifying		
50:1,3,9,10,17 51:6,8,	79:18 80:3,10,12,23		
11,14,18,20,24,25 52:1,			
9,11,16,18,19,20 53:8,			
13,14,15 54:1,2,3,5,17			
55:5 56:24 57:10,22			
58:1,2,8,9 60:11,14,15,			
17 62:6 63:5,7 73:11			

THE SULLIVAN GROUP OF COURT REPORTERS

5,9,11 71:10,21,24 72:20 73:12,19 75:8,20 76:17,20 77:1,5 79:17 80:22 85:16,23,25 86:2, 3 90:25 91:13,18,25 93:6	62:5 72:9 73:3 76:22 92:12	E	encrypt 39:10,19 42:5,13 43:21 46:9 51:25 63:2,12 86:14,18,20
Dick's 70:17 91:7 92:4,22	discussing 48:19,25 61:22	earlier 74:24	encrypted 22:8 24:3,24 26:20 39:4 40:4 42:15 43:2,4 44:3 46:20 47:10,13 83:20, 23 86:13,21,24 93:24 94:1
dictated 40:24	discussion 55:25 65:22	early 38:17	encrypting 31:8 39:18 42:21 62:16, 24 63:4
difference 72:19 74:12,15 76:19	discussions 90:18	easier 92:7	encryption 25:14 26:4 30:13 37:13 38:6,8 39:9,14,22,23,25 40:1,5,9,19 41:15,21,24 42:1,3 46:10,21 48:12, 16 50:9,14,20 52:1 61:13,22 62:6 63:3,6,23 80:8,15 82:11 83:11,15 86:7,9,12,25 87:3,5,7, 21 91:7,15 92:4,10,17 97:2,5
differences 74:17	disseminated 20:18	Eastern 64:9 90:1	encryptions 62:8
digging 64:17	distinct 56:1,3	effort 12:12,15,21	encrypts 86:16
directly 23:16	division 18:6	either/or 78:2	end 12:18 97:10
disagree 22:18	doctor's 29:1	elaborate 17:17 25:22 41:9 96:16	Endless 38:18
disagree 22:18	doctors 49:11	elected 41:25	enforcement 83:4
disagreement 22:16	document 64:15 65:1 79:20	electronic 7:19 95:13	engine 86:18
disclose 79:17 89:24	documents 7:20,23 11:4 12:10 13:18,22,25 14:3	embodiment 32:13 33:10 35:11 36:3, 6 42:20 46:24,25 47:11 48:1 77:1,5,12 84:22 86:8 87:7 94:24 95:17	ensure 7:5 82:12
disclosed 33:4 53:4 54:8,25 56:7 58:5 63:24 64:1 71:3,23 75:19 84:7 89:8,11	DOD 18:10	embodiments 28:23 31:2 32:19 34:5 44:10 46:4,5 51:22,23 52:8 53:7 58:5 95:18,24	ensuring 19:14
discloses 37:9,17 46:8 47:21 48:11 49:12 69:15 70:23 76:17,20 86:5 89:18 91:18	domains 49:21	employed 17:6,23	entails 17:18
disclosing 56:11 76:21 97:2	dozen 15:4,14	employee 17:24	entire 31:18 38:14 39:19 95:21
disclosure 30:23 31:4,15 32:15,21 33:7,10,24 34:5,9 37:25 38:1,9 42:23 44:6 50:8 51:21 54:16 55:3,6,8, 16,17 58:7,16 59:22 62:3 69:1 75:7,22 77:14 88:21 89:11	draft 97:7	empowered 82:14,19 83:3	entirety 27:6 64:24 69:24 81:12 94:13
discuss 45:22,24 97:19,21	drafted 12:25 13:5	enable 47:24	
discussed 50:4 51:5 53:16 61:12	drink 66:20	enabled 46:5	
	drugs 58:24	encompass 24:24	
	duly 6:4	encompassed 48:23	
	duration 7:22	encounter 27:8 65:3 70:1 81:14	
	Dyncorp 18:1,6,8,11,23		

THE SULLIVAN GROUP OF COURT REPORTERS

entities 20:25 21:2,4,5 28:10,17 29:2,8,11 35:15 36:8,18 46:17 49:5,9,13,16 51:9,11,12,14,24 54:2, 18 55:13 56:7,12 57:19 59:16 82:14,19 83:3,6 88:1 entity 20:19,22,24 21:10 28:9, 16,24,25 29:5,16,18,24 30:3,4,16 32:9 47:1,22 48:3 49:25 51:19 52:16, 19 53:18,21 54:4,6,12 55:4 57:3,5,6,7,18 74:7 78:22 79:5,9 88:4 environments 77:11 equal 69:5 errors 14:16 escape 36:24 essentially 18:5 86:22 87:23 EST 90:14 97:16 98:14 estimate 13:4,6 evaluated 19:19 Evenhaim 10:1 26:23,25 27:3,6,8, 11,17,20,24 28:20,22, 24 29:25 30:9,23 31:4, 13,15 32:16,18,25 33:3 34:12 37:8,9,16 38:22 40:7 41:23 43:14 44:4, 6,8 45:25 46:4,8 47:20 48:10,16 49:9,12 51:22 53:4,12 54:1,9,17,25 56:4,6,11 58:2,6,7,16 61:8,18,25 62:3 63:24 69:20 73:3 79:12 93:4 96:24 97:3,7 Evenhaim's 50:8,10 56:1 Evenhaim/settimi	97:6 evidently 67:11 EXAMINATION 6:8 examining 66:2 examples 28:16 31:7,24 34:11,15, 25 53:12,25 54:24 58:22 73:19 74:1 excluded 16:10 Excuse 66:20 Exhibit 9:2,21 10:2,6,10,16 13:18 16:13 25:8 26:23 64:14 69:17 81:4 94:9 exhibits 9:16 exist 14:17 56:5 88:20 existed 39:2 expect 75:2,14,23 experience 13:25 21:5 expert 11:13 12:2,16 14:24 explain 27:20 62:20 67:4 explained 33:13 89:15 explaining 34:2 explains 66:25 89:20 explicit 55:16 59:22 69:1 75:22 77:16 explore 14:11	express 54:16 55:3,6,7,17 58:7, 16 expressly 54:8,24 extent 20:16 30:5 37:3 88:7 F face 44:23 facets 47:24 facilitate 35:12 facilitated 48:13 fact 56:4 57:3 factor 15:23 factors 26:5,15 facts 40:16 fair 76:23 False 89:15 familiar 26:25 38:16 64:19 81:6, 17 94:11 feature 83:10 fed 39:15 feel 65:23 field 14:1 69:1 81:24 82:5 fields 40:23 43:4,10,12 51:3,6 55:14,20 figure 25:25 28:3,8,16 29:15	30:7,8 32:2,5 35:22,24 36:6,16 37:6 42:9,12 43:1,24 44:11,18 45:3 56:22 58:23 59:3 60:3 70:11,13,21 77:2,6,9,10 78:5 84:1,6,25 87:25 88:11,16 91:16 94:19, 22 95:1 figures 27:23,24 34:4,9 file 12:9 23:9 24:10,17 37:10,12 98:11 filtering 18:16 final 24:21 36:14 66:24,25 67:15 98:4,7 find 19:21 27:22 33:10,14, 18 68:25 77:15 finding 80:7 fine 33:24 45:15,18 64:7 firewall 78:12 Fish 6:12,15 fits 41:8 five-minute 45:14 64:5 fix 82:23 flows 88:19 89:4 93:19 focus 83:8,12 focused 40:4 focuses 53:5 folder 7:21 9:23
--	---	---	---

THE SULLIVAN GROUP OF COURT REPORTERS

follow 93:6	12 71:9,20 92:15 96:3, 6,20	68:6 69:5,11	18:14 19:14,18,22 20:11,14,20,25 21:2,5 29:6,8 30:4,16 48:9 49:24 50:1 51:12 56:23 57:4,11,18,25 59:19 60:4,6 62:17 74:7 80:25 88:1,4 92:16
force 26:22	functionally 30:12	group 22:9 24:15 25:15,19 26:7,17 67:24	HIPAA-COMPLIANT 19:1
forced 67:13	functions 32:23 33:12 34:7 47:5 48:20 50:21 70:24 71:23 72:4,11 76:23 77:13 85:20,22	guarantees 20:15	HIPPA-COMPLIANT 18:12
foregoing 24:23		guess 13:7 39:25 53:23 76:13	history 12:9 23:10 24:10,18 60:20
form 28:11 30:17 35:3 39:22 44:21 47:3 52:22 63:8 66:12 78:18 93:10	G	guidance 56:22	hospital 29:1
format 73:7 75:4	gathering 50:6	guide 17:8,12,20,22	hospitals 49:11
formats 74:25	Gaussian 67:1,5,12	Gupta 6:15	hour 7:11 15:17 45:12 90:8
formatted 72:21,24	gave 59:24	guys 21:6	hours 11:3 15:24 90:7 98:4
formatting 72:16 75:9,12,20	general 7:11 20:23 35:12 41:24 79:13	H	HP(I,J) 44:15 45:6,8
formed 22:17 48:20	generally 37:17 42:24 51:13 70:13 80:19	happen 7:16 33:1,2	
forming 13:19,23	generate 52:3 86:12	happy 65:16 90:8	
forward 62:9 73:8	generated 24:4,5 58:12	harder 79:11	I
forwards 78:8	generates 36:11	hash 26:1,3,6,8 80:7	ID 32:3 47:16 83:20 86:13 93:24 94:1
found 33:15 56:8	generating 86:19	hashed 26:12	idea 91:22
Foundation 44:21 91:9	generation 86:18	hashes 38:12	identifiable 29:3 57:12
founded 19:8	give 8:12 73:24	health 28:5,15	identification 48:12 53:24 77:17
free 65:23	good 6:9 27:16 64:5 65:12 70:8 81:20 90:3 98:11	healthcare 18:20 19:4,10 57:22,24 82:6 84:21	identified 11:8 13:23 17:10 67:24 74:3 83:13 84:24 85:2, 8,12,17 88:11,23 89:14, 18
front 12:13	government 18:10	held 16:21	identifier 22:25 44:15,19,24 45:2, 7,10 46:20 47:13 48:8
fulfill 85:20	granularity 61:15	helpful 58:22	identifiers 44:1 45:9 47:10 48:5,6
full 8:5	Great 9:25	high-level 70:24 84:8	identify
function 44:10,25 47:23 48:3 51:2 54:7,13,21 67:2,5,	greater	higher-level 72:23	
		HIPAA	

THE SULLIVAN GROUP OF COURT REPORTERS

31:14 32:15 33:7 34:14 50:11 52:20 53:13 58:22 59:8,12 identifying 24:24 46:9 56:25 identities 52:9 identity 23:1 25:15,19 26:6,16 46:13 52:17 57:13 IDS 52:3 80:18 illustrates 77:10 imagine 58:13 immediately 14:6 implement 38:14 46:23 76:25 79:1, 4,8,14 80:11,22 82:11 88:10 91:7 implementation 18:12 19:1 31:21 36:23 39:6,24 implemented 32:11 87:19 implementing 42:8 64:2 78:13 import 96:3,6 important 29:10 impossible 11:14 12:5 Inc./paul 16:18 inclined 56:9 include 22:7 31:16 32:4 35:5 37:13,17 40:14 43:10, 12 56:24 60:15 74:1 80:14 92:10 96:11,13, 18	included 16:13 60:22 includes 30:13 31:25 39:11 42:4 43:18 59:18 72:7 84:13 87:15 89:14 93:24 96:2 including 35:1 41:15,25 incompatible 40:6 incorrect 23:5 index 9:18 indication 68:18 individual 22:25 23:1 46:12,13,21 47:9,12,19 48:12 50:11 52:21 53:10 57:14 59:6, 10 63:4 66:8,16 87:20 individual's 31:6 47:24 48:4,7 individually 22:23 individuals 20:15 25:15,19 26:7,16 29:12 41:25 42:4 48:13 52:10 59:13 66:16 Indranil 6:14 infeasible 25:21,23 26:9,11,22 inference 67:19 inferring 88:25 89:2 information 22:8 23:20 24:5,15,24 26:14,20 29:11 47:18 49:3 50:15 56:25 57:12, 13,24 58:3 59:5,6,15, 18,23 60:2,3,7,17,22 66:3 70:14,18,19 73:9, 10,13,17,20 74:4,6,9, 13,20 76:10 77:22 85:16,19 86:1 91:22	92:21 93:14,21,23 97:4 instance 41:18 82:24 institutions 21:8 instrument 17:19,21 insurance 21:7 50:5 intake 74:14 integrate 91:14 integrity 37:25 38:2,10 intent 38:23 86:8 inter 6:23 9:7 interest 21:9 59:9 interested 36:4 interesting 95:22 interface 36:10 interim 46:5 interior 40:3 internal 52:6 internet 71:5 78:11 81:2 interrupt 7:6 intranet 71:4 78:11 invention 9:13 56:1 81:25 82:4,5, 10 83:14 invite 31:23	involve 17:13 involved 15:8 18:11,15,20,25 19:14 27:13 involvement 27:12 65:7 70:6 81:18 involving 6:24 22:4 IPR 6:24 7:20 9:6,8 11:12, 17 27:12 81:18 94:16 IPRS 12:3 15:7 issue 17:16 items 40:23 J January 17:25 Jeffrey 6:15 joined 6:14 July 16:22 17:25 21:25 Justin 6:19 K Kerberos 14:5 key 39:9,12,14 46:10,21 47:23 48:2 52:1,12 82:11 83:20 86:14,16, 18,21,22,23 87:15,18 88:8,18 key-based 86:10 key-management 86:11
---	---	---	--

THE SULLIVAN GROUP OF COURT REPORTERS

Keyed 38:12 keying 26:13 keys 42:6 61:14 83:17 86:20 87:21 kind 40:1 knowing 47:22,23 48:2 knowledge 16:3,6,9 80:9,25 94:15 L labeled 9:23 10:8,12,13,18 85:7,8 laboratory 74:3 Landi 81:3,6,9,12,14,18,21,23 83:8,13 84:7 86:5,9 87:1 88:21 89:12 90:25 91:18,24,25 92:14 93:1, 2,14,23 Landi's 91:7 92:4,23 language 25:13 larger 20:2 law 29:13 49:4 83:3,4 layers 39:23 left-hand 29:19 66:19,24 legally 82:14,19 83:3 length 73:3 level 41:24 42:1,3,7 61:7,10, 17 62:4 86:15	levels 40:20 49:19 61:13 libraries 81:1 lieu 92:24 light 42:23 likewise 79:7 limitation 65:15 66:15 68:25 limiting 69:1,9 lines 37:8 40:7 41:22 link 46:11 47:8 53:9 57:23 linkage 47:22 48:3 linked 53:22 linking 96:18 list 13:18 15:2 19:21,24 31:17,25 32:3 34:25 35:10,14 41:25 42:4,13 43:7,23,25 44:2,15,19, 24 58:2,14 59:23 60:23 listed 20:8 74:5,15 lists 31:8,10,15 44:20 45:2,5 litigation 14:24 22:4 LLC 6:13 8:22 16:18 17:2 located 32:16 33:5,8,20 86:25 locations 48:11 long 25:24 65:1 92:19	longer 45:16 74:16 90:5 looked 12:11 65:1 lots 28:23 31:13 96:13 lunch 7:12 90:3,16 M made 98:11 main 91:22 maintain 29:2 51:15 84:23 85:17 maintained 52:16 54:3 maintains 95:12 make 6:17 14:1 45:15 52:5 89:5 93:12 96:19 makes 36:13 management 39:12 52:12 88:18 manager 74:2 managers 28:5 mapping 97:5,7 maps 85:23 marked 9:1 Maryland 8:9 Massachusetts 22:5 master 87:15,18 88:8 match	24:6 43:4,20,22 47:16 53:13 54:2,7,13,20 63:2,11,17,21 matched 43:10,13 51:4,5,6 87:13 matching 30:13 50:11 51:24 52:2, 18 54:17 55:5 56:7,11 62:15 material 11:8 matter 22:16 23:6 24:2 matters 12:3 14:25 27:14 meaning 21:23 24:19 25:4 meaningful 51:3 73:4 means 25:24 26:22 52:7 mechanisms 80:5,20 medical 17:8,12,14,22 18:12,19 19:1 20:16 22:8 24:14 29:11 31:6,11,16 32:1,4 34:13 35:1,6 57:10,23 58:3,8,14 59:6,18,23 60:2,14,15,17,20,22 70:14,18 73:9,13,16,20 74:6,9,13,19,20 76:10 77:22 85:16 86:1 95:13 medication 59:13 60:6 medications 59:5,8 60:8 meeting 10:21 meetings 10:24 memory 13:13 23:19 56:13 mention 46:16 mentioned
--	--	--	---

THE SULLIVAN GROUP OF COURT REPORTERS

74:24 merger 46:5 48:12,16 merging 96:11 message 38:13 39:4,18,20 40:1 63:6 method 77:11 methodologies 80:10,12,14,23 methodology 80:3 methods 79:17,21,23 82:10 microdata 29:3 34:23 35:5 36:20 mind 14:6 35:17 mining 21:9 minor 20:1 minutes 45:17 58:21 90:10 97:11 MIR 73:16 74:16 75:11,17, 20 76:1,9 77:2,6 78:2 85:19 92:25 modification 92:22 modified 38:4 modify 68:4 91:13 modifying 92:9 module 32:6,8,16,22 33:4,8,20 44:13,14 moment 50:6 65:22 73:24	money 21:6 months 13:10 morning 6:9,10 motivation 42:21 move 33:25 76:23 77:13 multiple 39:23 45:2 46:19 58:5 61:13 62:8 70:21 91:19 Murphy 10:15 64:13,19,21,24 65:3,7,13,18 66:1,4,25 67:8,17 68:3,10,11 69:3,12,20 Murphy's 66:9 N named 20:3 names 57:9,14,19 58:25 62:17 63:5 nature 12:14 18:7 necessarily 14:21 30:3,15 32:23 34:7 39:21 43:3 46:22 56:3 60:16 67:16 needed 7:12 82:15 network 18:2 23:20 39:19 41:6, 10,17 networks 36:22 Nick 6:11 noncovered 57:5,7,18 78:22 noon 64:9	normal 15:17 notes 40:7 41:23 48:16 50:6 number 9:16 15:24 31:9 39:7 40:19 42:22 48:20 66:10 67:11,24 68:7,11, 12,15,17,21,23 69:2,4, 10,11,12,13 77:18 80:4 81:1 82:21 numbered 85:7 numbers 38:18 numerous 48:11 O oath 8:10 obfuscate 66:5 67:6 obfuscated 67:23 68:6,11,12,15,17, 21,23 69:4,13 obfuscates 67:23 obfuscation 68:5 Object 35:3 Objection 28:11 30:17 40:16 44:21 47:3 52:22 63:8 66:12 91:9 93:10 occur 10:24 32:24 48:17 49:1 51:24 53:18 54:22 55:6 62:6 75:15,16 occurred 53:20 occurring 41:21 occurs 54:5 87:3	October 98:5,8 offer 67:21 offering 16:4 office 29:1 74:3,5 Oliver 6:19 28:11 30:17 40:16 44:21 47:3 52:22 63:8 66:12 91:9 93:10 97:24 98:10 one-way 26:1,4 operated 28:4,9 84:20 operations 17:3 36:16 opinion 16:4 22:17 23:7 42:18 opinions 12:17 13:20,24 14:7,12 16:7,10 option 71:4,5 92:9 options 71:3 order 24:12 31:3 43:21 51:2 54:20 56:23 63:2,17 83:5 98:3 ordinary 9:12 21:22 24:19 organizations 84:21 original 26:12 output 67:1,13,18,22 overview 84:6 owner 6:13 8:21 owners
--	---	--	--

THE SULLIVAN GROUP OF COURT REPORTERS

82:13,18	43:7,23 44:2,15,19,24	periods	place
owners'	45:2,5,7,8,10 50:12	74:16	32:11 47:4 92:4,15
22:4	51:20 53:9,15 57:9,19	permit	places
	58:2,13 59:22 60:23	53:9	33:1 48:21 50:5 53:6
	62:17 63:5 74:4 76:14	person	plain
P	77:6,18 78:15 79:18	9:12 18:5 42:25 47:15	24:19
p.m.	82:12,13,18 83:12	54:14 60:5 79:22 80:11,	plan
64:11 89:25 90:14	84:10,13,19,23,24 85:2,	21,24 89:2,22	28:15
97:16 98:14	6,8,12,15,17 86:5,6,13	personally	plan/pharmacy
package	87:1,6,9,10,11,22,24	56:25 57:12	28:5
16:12	88:3,12,22,23 89:13,14,	perspective	play
paper	18,19 92:23 93:8 95:5,	19:6,23 32:4	52:13
19:21 20:4,7,9	10,15,19 96:8,11,12	pertain	plug
paragraph	patient's	47:15	91:18 92:7,14
15:15 21:14,16,17 22:2	34:13 52:17 60:14,20	pertains	plugging
24:22 37:16 41:22 46:3	83:19	55:25	91:25
56:17,21 61:1,6,18	patient-level	Petitioner	plural
62:1,9,14 66:19,23	29:3 36:20	6:17,20 8:17 22:20	45:4
73:19 77:21 80:1 90:21,	patients	pharma	point
24 91:5 92:3 96:9,10	31:16 43:25 51:15 58:3	21:8	19:2 33:16,24 51:16
parameter	59:5 60:7 66:10 67:24	pharmaceutical	54:1,18 55:7 59:2 64:5
41:25 42:4	82:15,20 83:9	28:4 29:14,17,20 36:7	89:12
parameters	patients'	37:5 58:23 59:4	policy
66:11	31:11 32:1	pharmacy	18:15 19:16 40:24
part	Paul	74:2	portion
32:8,22 34:8 58:25	6:3 8:7	phrase	43:14 55:18 59:3
59:7,23	PBM	9:6	portions
partes	28:15	physical	12:19 40:3 46:9 56:6,11
6:23 9:7	PCP	77:10	POSA
pass	95:12	physician's	9:11 21:24 24:22 56:22
97:23	PCPS	74:2,5	POSITA
passed	94:25 95:2,5,7,15	PII	9:11 54:23 78:21
74:23	people	18:21 19:5,11 20:17	position
passing	18:15 38:5 53:1	29:7,22 30:6,19,21,24	34:10
85:19	percentage	31:2,5,9,22 32:19	positions
past	12:24	33:11,18 34:6,12,21,24	16:21
15:10 36:24	Perfect	35:5,21 36:13,24 37:4	possession
patent	98:9	48:8,25 49:7 51:15,25	29:22
6:13,24 8:21,25 9:1,2	perform	53:5 55:14 57:6,8,9	possibilities
12:9 14:8 22:3,5 23:10,	50:10	63:12,22 66:17 67:19	31:13 51:22 69:14
14,24 24:8,10,25 25:7	performed	74:8,11 76:15 79:16	76:18
26:19 61:7	33:12 48:20 54:17	80:18 85:14,24 86:16	possibility
path	92:17	88:2,7,15,19 89:5,16	58:20 68:1,13,24 69:12
93:6	performing	92:19 93:1	76:19 77:20 78:23
patient	47:22 50:9	PII-CONTAINING	
30:2 31:8,10,15,25 32:3	performs	91:23	
34:25 35:10,14 42:13	48:3		

THE SULLIVAN GROUP OF COURT REPORTERS

potential 33:1 power 90:9 precluded 16:3 preferable 37:17 40:9,14 42:24 preferably 37:12 preferred 77:10,11 preparation 11:4 prepared 10:19 12:8 preparing 11:2 12:15 14:4 27:3 64:21 69:21 81:10 present 56:1 65:7 70:6 82:3,9 president 16:17 pretty 26:18 44:25 65:1 prevent 37:24 38:8 67:19 primarily 11:7 18:10 prior 10:22 55:25 privacy 19:14 20:11,14 47:25 48:4,7 50:1 55:14 82:6, 12 83:12 privacy-identified 55:20 privacy-sensitive 34:22 35:4 private 29:11 86:23 87:15,18 88:8 problem 63:23 82:22	procedure 57:24 58:14 procedures 17:15 proceeding 6:24 9:2,7,8,21 12:8 27:4 65:8 69:22 70:6 proceedings 98:13 process 12:7 50:5 52:25 53:3 70:17 processed 33:18 35:1 79:16 processing 32:19 34:6 46:11 47:2 75:14,16 84:11,14,19, 23 85:6,15 86:6,13 87:1,6,11,24 88:3,13,22 89:13,19 92:24 93:8 96:15 processor 23:19 25:14 48:17 processor's 48:18 produce 39:16 46:20 52:1 73:5 86:6 produced 93:21 produces 68:11,22 95:10 producing 25:10,11,13 products 17:15 projects 11:20 18:8,9 prompted 25:3 prop 17:1 proposed 92:4 93:16 proposing 91:6,13 92:23	protect 29:7 39:2 40:20 41:17 49:3 55:13 protected 60:6 85:14 92:19 protecting 19:5,11 83:12 protection 42:7 82:6 protections 60:4 protocol 38:25 39:11 51:7 72:22, 25 protocols 38:20 provide 13:12 22:15 38:6,11,19, 22 41:5 42:7,16,24 43:2 44:3 49:13 59:22 61:16 69:12 76:4,6,9 provided 9:24 12:11,17 13:18 14:5 20:17 23:12 27:10 36:10 65:5 66:5 70:3 76:15 81:16 94:17 providers 95:5 provision 49:24 provisions 57:4,17 pseudonyms 80:18 public 86:10,14,16,21,22 98:11 publication 19:20 publications 20:2 published 19:21 put 7:21 12:12 13:4 32:14	Q queried 74:19 92:24 queries 39:2 43:17 50:25 51:3,8 66:15 71:11 87:12 query 36:11 41:18 42:13,15 43:1,3,8,9,12,15,16,17, 19 51:18 54:20 55:5 56:23 58:12 59:1,7,8, 14,17,23 60:9,11,13,19 66:1,2,6,9 67:25 69:4 72:16,20,21,24 73:4,7,8 74:18 75:1,4,9,17,20,25 76:5 78:4 93:2,5 97:4 querying 50:15,18 59:16 question 25:5 26:18 55:1 57:16 59:21 60:16,21 62:22 66:22 85:4 91:10 94:18 questioning 8:16 21:11 questions 7:7 27:21 65:16,21 69:19 91:3 97:12,22,25 quote 62:16 R randomize 67:5,11,12,17,22 randomizing 66:25 range 67:1 68:4,6,18 rate 15:17,20 re-ask 91:10 re-encrypt 40:2 reaches 78:16
---	--	---	--

THE SULLIVAN GROUP OF COURT REPORTERS

read 14:1,21 27:6 31:18 32:2 37:14 42:23 44:22,24 46:14 64:24 68:4,14 69:24 81:12	18:13 19:1 34:1,2,4 46:9 52:16 83:19 98:2	relation 18:22	16:1 40:17 77:3 83:22 96:21
reader 80:9	records 20:16 26:25 32:3 46:11 47:8,13 50:12 53:9 60:14,19 66:14 69:2 82:13,15,19 95:13 96:12	relax 34:18	requester 36:15 37:3,5
reading 43:1 80:2	recover 26:12	release 29:11 76:15 95:15,20	requester's 71:13,15,18,20,24 75:19 78:7,8,16 79:5 91:8,14,21 92:5,13,18 93:7,18 94:2
ready 64:3	refer 9:16,20 10:1,5,9,15 25:7 46:17 61:6	released 78:1 87:9,11	requesting 59:4 70:14,25 71:9,12 72:17 78:1,9,21 79:1 93:11,17 94:2
reason 8:12 23:4 27:19	reference 27:9 31:19 35:7 51:17 52:7,14 56:9 64:4,13 65:4 69:16 70:2 72:6 75:6 80:7,22 81:4,6,15 89:9 94:8,16 95:21,25	relevant 17:11	requests 23:21 70:17,19 72:16 98:2
reasonable 65:14 76:16	referenced 45:3	remedied 14:22	require 34:7 41:7 60:4
reasons 79:6 82:21	references 10:23 11:6 12:10,11	remember 75:22	required 67:16
recall 11:11,14,15 12:3 13:2 14:4 20:6 27:11,13 72:3,5 95:23,25	referred 43:23	repeated 62:16,23 63:3,23 66:15	requirements 49:20,22 61:23
receipt 73:8	referring 8:17,22 9:1,7,12,19,20 10:1,5,9,15 21:12 43:15 45:8 57:9 59:3 67:9 77:25	rephrase 57:16	requires 41:9,11
received 7:19 52:18 53:14 54:2 72:16	refers 40:12 43:16 46:4	replace 91:21	requiring 37:9,11
receives 49:25 52:10 74:25	reflects 32:13	replacing 91:23	reread 10:22
receiving 37:11	regard 38:10	report 95:10	research 11:19 21:8
recently 12:6	regulations 21:1	reporter 16:1 40:17 77:3 83:22 96:21 98:1,6,9	residence 8:8
recess 45:20 64:11 90:14 97:16	reidentification 83:9,13,16,18	repository 73:10,17,20 74:6,14,21 77:22 85:12,16 86:2 88:12	respect 22:3 24:14 69:20
recites 25:13	reidentify 82:14,20 83:7 87:22	representations 28:3,8	respective 34:22 37:11,13
recognition 17:19	related 21:20 46:12 47:9	represented 85:25	response 23:20 27:21 67:25 69:3 70:19 76:4,9 78:4 93:6, 16
recollection 28:22 30:25 61:20 65:6 70:5 72:1 79:20 81:17	relates 82:4	request 36:9 63:5 66:11 71:13, 17,22 72:19,22,23 73:8 74:25 75:4,9 92:13 93:13	responsibilities 16:24 18:4
reconvene 64:8 90:11		requested	responsible 12:22 17:2 29:5 72:15
record 7:5,18,20 8:6 9:18			restart 66:22

THE SULLIVAN GROUP OF COURT REPORTERS

result 66:9 67:23 68:22 76:1	17 94:2	21:19 66:4 81:24 82:3	11:12
results 36:12 41:19 66:5 67:6, 21 73:5	routes 71:22	secure 18:16 34:20,21 40:22, 23,24 41:14,16 49:8	server 22:7 23:18,24 25:14 30:12 31:21 36:9,10,11 37:2 41:14 59:14 71:14, 16,18,21,22,24 72:8,11, 12,15 73:4,7 74:15,19, 24 75:8,19,25 76:2,7,10 77:7 78:7,8,12,16 79:5, 8,11 88:8 89:5 91:7,8, 14,15,20,21 92:5,8,10, 13,17,18 93:7,18 94:3 97:2,5
retained 14:24	routing 91:22 92:13	secured 35:21 82:11	servers 76:24 85:24
retrieving 70:14	rule 19:15 20:11,14 50:2	Securemethods 16:18 19:4,7,8,10	set 42:13 52:24 84:10
return 53:8 66:14 67:20 70:18 76:1 77:22 92:20 97:14	ruled 52:7	securing 53:5	Settimi 10:5 94:8,11,16,20 96:23 97:1
returned 69:2	run 17:1	security 19:18 36:25 37:1,2,18, 21,23 38:7,11,17,19,22 39:5 40:15,21 41:4,5,10 42:16,25 43:2 44:3 47:6 48:21,22,24 49:6,18,19, 20,22 52:25 61:7,11,17 62:4 63:7	shorthand 73:12
returning 40:8 68:6	S	security-related 18:9	showing 58:23 72:10
returns 68:18 69:3 77:6	S-HTTP 38:20	seek 36:24	shown 28:16 30:7 32:5 34:9 35:23 36:6,16 71:7 77:1 84:25 88:11,16,17 94:22,25
reveal 23:1	S/mime 38:20	seeking 67:19 68:25	shows 28:3,8 84:10
reversible 83:11,15	Sarkar 6:14	select 43:18	shut 8:1
review 6:23 9:7 11:4 22:11 24:8,17 27:3 31:23 64:21 65:23 69:21 81:9 95:21	satisfy 66:10 93:14	send 35:14 41:6,10 59:15	sic 66:23,24
reviewed 11:9 12:9 23:9 94:13	scanned 64:25	sending 37:4 53:21	side 29:19 47:6 48:17,18,21, 22,23 55:4 63:19 66:19 68:2 75:10
reviewing 14:4	schematic 42:20	sends 36:9,14 75:25	signed 78:18
Richardson 6:12,16	scheme 39:9 52:12	sensitive 18:17 35:13 37:4	similar 52:3 73:2 93:6
right-hand 68:2	schemes 38:15,17 40:19 41:3	sentence 56:21 68:16	similarly 14:19 22:8 24:3,14 73:16 79:3
Rishi 6:15	scientist 18:1	separately 44:19	simply
role 18:4 52:13	scope 26:19	separation 53:1,3	
roles 16:25	scroll 73:22	September 6:1	
rough 98:4,5	search 30:1 35:20 55:10 56:9 58:19 66:11 72:1 79:19, 24	series 35:23	
routed 71:15,17 78:4 93:3,13,	searched 58:10	served	
	searching 35:12 75:13		
	section		

THE SULLIVAN GROUP OF COURT REPORTERS

23:7 63:4	53:8,13 56:24 58:2,9 73:11 93:2	11,17,19,21 47:7 53:2 63:14 64:3,8,12 66:18 77:4 83:25 89:25 90:10, 13,15 91:12 93:15 96:22 97:9,14,17,22 98:3,7	support 77:21
single 55:21 66:16	speaking 7:6 51:13 80:19		supported 56:4
sir 8:4	Special 47:21	steps 35:23 36:2	supports 50:9
sit 34:18 58:18	specific 14:3 20:21 34:11,14 40:23 53:12,25 54:24 57:20 79:20	stored 60:11	surveillance 84:16 87:14
sites 84:20 96:8	specifically 18:19,22 43:8 63:25 68:14	stores 74:3	sworn 6:4
sitting 11:11 72:3 95:23	specification 23:9 24:9,17 31:23	storing 54:11,19 63:20	symmetric 86:19 87:20
situation 41:20 58:13,17	spend 11:1	stream 39:16	system 18:13 19:2 30:7 42:12 43:5 49:2 51:2 52:24 54:7,21 61:15,23 64:2 70:13,17,22 72:7 73:9, 14 74:10,13,20 75:3,16 76:22 78:13 79:1,4,8,15 84:7,13,14,16 86:7,9, 11,12 87:11,14 88:4,13, 23 89:13,19 91:24 92:4, 14,16,23,24 93:8,13 95:8,20 96:2,20
size 41:8	SQL 43:18	streaming 40:5	systems 24:12 28:4,9 39:22 42:8 52:4 56:3 75:15 76:25 82:10 84:11,19,23 85:6, 15 86:6,13,25 87:1,5,6, 8,24
skill 9:12 31:20 40:25 42:25 54:10,14 79:22 80:11, 21,24 89:10,22	SSL 38:18 39:2	streaming-level 38:19	
slightly 24:1	SSL-LEVEL 40:5	string 39:15	T
sole 17:1	stake 21:8	stronger 42:1,3	table 13:23
solution 66:24,25 67:15	standard 38:24 43:17	strongly 41:23	taking 6:12 60:5,8
solutions 18:2 67:20	start 34:19	structure 96:14	talk 36:5
sort 51:16 70:23 75:12	starting 46:7 55:12 82:8	stuff 12:17,18	talking 26:19 29:17 73:6 88:7
sorts 37:25 38:20 39:12 96:15	starts 21:19	subject 20:25 35:6 50:1 82:14	talks 34:6 55:19
sought 59:19 60:18	state 8:5,8 21:22	submit 71:13	target 17:21
source 28:10,16,24 29:2,5,11 32:9 35:15 36:18 46:17 49:12,16 51:8,11,14,24 52:16,19 53:18,21 54:1, 3,5,12,17 55:4,13 56:7, 12 57:3 60:11 62:6	stated 14:12 24:25	submitted 14:14	targeting 17:20
source-entity 48:18	statement 62:20	submitting 71:11	
sources 34:21 46:8,16,20 49:1 50:10 51:6,25 52:6,9	step 25:10 37:9,11 42:12,16 43:24	substance 45:23 90:19 97:20	
	Stephens 6:8,11,22 16:2 28:14 30:22 35:3,8 41:2 45:1,	suite 17:15	
		super 39:22,25 41:21 61:22	

THE SULLIVAN GROUP OF COURT REPORTERS

team 97:12	times 14:23 15:1,4,5,6,12 42:6 55:2	true 58:18 67:24	23:24 24:16 27:16 29:9 35:9 36:1 37:20 43:9,15 44:8 45:6 50:7,10 55:23 65:12,14 67:8 68:10 70:9 81:21 91:4
technical 18:5 19:6,16,22 81:24	titled 81:24	trusted 79:13	understands 88:17 89:23
techniques 80:16	today 6:13,23 8:10,13,16 21:11	truth 6:5,6	undo 82:22
technology 27:17,20 65:13 70:9 81:21	today's 10:20 11:9	truthful 8:13	unit 55:21
telling 32:25 77:14 89:3,21	token 22:7,24 23:13 24:23 25:2,4 26:2 30:13 50:11 51:24 52:17,18,20 54:2, 3 55:15,17,19,21,23,24 57:2 62:15 63:1,11 91:17,24	turn 21:14 26:23 27:23 35:22 45:25 56:14 64:13 65:17 69:16 70:11 81:3 84:1 90:21 94:8	user 36:9
tells 29:13 69:9	tokenization 54:5	type 60:3 75:12	V
ten 15:3,9 45:17 64:7 97:11	tokens 24:4 25:14,16,20 26:17 31:1,3 35:19,20 52:2, 10,15 53:8,14,22 54:11 55:4 61:14 63:11,20	types 21:4 80:18 93:12	values 68:5
term 8:25 21:10 23:24 24:17 43:16 63:11	tool 66:1,2,6,9	typically 39:4,8 49:11	variety 88:9
term's 21:22	top 44:14 87:25	typos 14:19,21	Venable 6:19 11:23,24 12:1
terms 8:15,17,21 22:3,7,11 38:3	total 71:25 72:5 95:25	U	versed 89:3
testified 6:6	transcribed 7:3	U.S. 6:24 9:2	view 25:18 50:8
testimony 8:13 45:23 90:19 97:20	transcript 98:1	unable 89:12	viewing 71:1,10,12 72:17 78:22
text 34:5,9 39:17 89:12,17	transition 64:4	unattainable 25:15,20 26:7,17,21	Vigilytics 6:13 8:22
things 28:12 33:1 37:25 39:12 41:11 42:5,22 43:18 49:11 53:1 61:22 70:20 72:18 80:14 96:13,18, 19	transmission 37:18,21,23 38:7,11,16, 22 39:5,19 41:4 42:16, 25 43:2 44:3 63:7	unauthorized 37:24 38:1,4,8	violate 57:23
thinking 79:25	transmit 58:2 60:17	unclear 91:11	violated 57:5,18
Thursday 6:1	transmitted 36:17,21 58:15 74:18	understand 6:25 7:2 8:10,19,23 9:4, 9,14,22 10:3,7,11,17 16:17 18:1 20:19 21:11, 24 24:23 26:20 28:15 31:20 34:3 35:5 43:1,25 46:19 54:23 55:21 56:22 59:25 60:24 62:7, 22 63:11 64:2 69:7,8 73:12 78:6,21 85:4,13 89:11,22,23 91:6	violation 57:25
time 7:10 8:3 9:13 11:1 14:13 15:16 39:20 55:2 63:1 74:16 90:3	transmitting 37:10 57:5,19 58:8	understanding 20:10,13,23 21:24	violations 37:25 38:2
timeframe 13:11 17:7			virtue 88:19
			vitae 16:14
			W
			waiting

THE SULLIVAN GROUP OF COURT REPORTERS

33:14

wanted
50:16

warehouse
95:8,16,20 96:2

water
66:21

ways
25:1 35:17 38:14,20
39:7 40:20 41:15 49:15
53:6 57:15 67:11 88:10
91:19

week
10:24

wider
68:4

window
7:25 8:3

word
55:19,22

work
12:1,16 15:22,24 17:12,
17 18:19,23 19:13
24:12,13 54:6 75:2,24
78:14 86:9 90:9 92:8
94:16

worked
11:22,24 12:5 17:4 18:8

working
13:8

works
92:12

wrap
90:8

written
12:20 34:5

wrote
12:17,18

Y

years
15:3 17:9