

1
2 UNITED STATES PATENT AND TRADEMARK OFFICE
3 BEFORE THE PATENT TRIAL AND APPEAL BOARD
4

5 DATAVANT, INC.,

6 Petitioner,

CERTIFIED COPY

7 v.
8

9 VIGILYTICS LLC,

10 Patent Owner.
11

12 Case IPR2024-00226 (US Patent No. 9,118,641)
13 Ref. 25412-0020IP1
14

15 VIDEOCONFERENCE DEPOSITION OF

16 DR. PAUL CLARK

17 January 16, 2025

18 Page 1 - 82

19 10:05 a.m. - 1:05 p.m. EST
20

21 REPORTED BY:

22 Tamara L. Houston

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

24 Job Number 146317
25

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 10:05 a.m. to 1:05 p.m. EST, Thursday, January 16,
2025, before Tamara L. Houston, CSR No. 7244, CCRR, RPR.**

1 **APPEARANCE OF COUNSEL:**

2

3 **On behalf of the Petitioner:**

4

VENABLE LLP

5

BY: JUSTIN J. OLIVER, ESQ.

NICHOLAS MARCELLO, ESQ.

MICHAEL SANDONATO, ESQ.

6

600 Massachusetts Avenue, NW

Washington, DC 20001

7

(202) 721-5423

joliver@venable.com

8

9 **On behalf of the Patent Owner and Witness:**

10

FISH & RICHARDSON, P.C.

11

BY: NICHOLAS STEPHENS, ESQ.

JEFFREY BARCLAYM, ESQ.

KARL RENNER, ESQ.

12

3200 RBC Plaza

60 South Sixth Street

13

Minneapolis, Minnesota 55402

(612) 335-5070

14

15

16

17

18

19

20

21

22

23

24

25

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

JANUARY 16, 2025

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

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

--000--

(Exhibits marked electronically.)

1 Thursday, January 16, 2025, 10:05 a.m.

2 --000--

3 COURT REPORTER: My name is Tamara Houston,
4 California Certified Shorthand Reporter Number 7244.

5 (Whereupon PAUL CLARK, having been
6 called as a witness was sworn to
7 tell the truth, the whole truth,
8 and nothing but the truth.)

9 --000--

10 EXAMINATION BY MR. STEPHENS:

11 Q. Good morning, Dr. Clark. Good to see you
12 again.

13 A. Morning.

14 Q. I believe this is our third deposition in this
15 or related cases, so introductions might not be
16 necessary. But as you know, I'm Nick, and I'll be
17 asking the questions today on behalf of patent owner,
18 Vigilytics.

19 Do you understand?

20 A. I do.

21 MR. STEPHENS: Would counsel for Petitioner
22 like to make his appearance?

23 MR. OLIVER: Justin Oliver on behalf of
24 Datavant Venable.

25 ///

1 BY MR. STEPHENS:

2 Q. Dr. Clark, you understand that you're under
3 oath for today's deposition?

4 A. I believe we just did that, yes.

5 Q. Is there any reason that you would not be able
6 to testify truthfully and completely in responding to my
7 questions today?

8 A. No.

9 Q. And you understand that we're here today
10 regarding the reply declaration that you submitted in
11 IPR 2024-00226 involving the '641 patent?

12 A. Yes.

13 Q. Do you understand that this exhibit -- or this
14 reply declaration has been marked as Exhibit 1015 in the
15 IPR?

16 A. I do not.

17 Q. If I represented that to you, would that be
18 your --

19 A. Yes.

20 Q. And this is the second declaration that you've
21 submitted in this IPR, correct?

22 A. Not sure that's true, but I'll accept that
23 representation as well.

24 Q. Are you aware that you submitted another
25 declaration in this IPR?

1 A. I am.

2 Q. And this would be your second declaration
3 submitted in this IPR?

4 A. As far as I know. I haven't been keeping
5 count.

6 Q. Your -- no other declarations come to mind
7 that you submitted in this IPR at this time?

8 A. Not sitting here today. I don't recall any.

9 Q. When I refer to your declaration today, I'll
10 be referring to the reply declaration that you submitted
11 last month in December of 2024.

12 Do you understand?

13 A. That's fine.

14 Q. How did you prepare your declaration in this
15 proceeding?

16 A. Same as the other ones. We had discussions.
17 I established my opinions, and then they were written
18 down by me and others.

19 Q. And who were the others?

20 A. I don't know. I know at least counsel here
21 today was involved.

22 Q. About how much of the declaration did you
23 draft on your own as opposed to leaving the drafting to
24 others?

25 A. The actual writing, I don't know. It was

1 probably an even collaboration. They have their
2 templates and other things that they like to write, but
3 I'm responsible for the opinions in the dec, just like
4 the last ones.

5 Q. Are you aware of any errors in your
6 declaration?

7 A. If I was, I would have fixed them.

8 Q. How did you prepare for today's deposition?

9 A. I had a call with counsel to go through my
10 declaration.

11 Q. About how many hours did you spend preparing
12 for the deposition?

13 A. A couple.

14 Q. And do you have any materials with you right
15 now relating to your declaration?

16 A. I have the files on my laptop. I do not have
17 them open unless you ask me to open them.

18 Q. You have no notes or other writings?

19 A. Of course not.

20 Q. Okay. And you're not in communication with
21 anyone outside of this deposition, correct?

22 A. No. Closed my emails and my text messages.
23 I'm all yours.

24 Q. All right. Thank you.

25 I may refer to a number of documents today, so

1 if you'd like, I will drop a few documents into the chat
2 that you can feel free to refer to as we're going
3 through questions.

4 So I will drop that in now.

5 A. And I'm allowed to download those, yes?

6 Q. Yes.

7 Are you able to open a zip file if I sent all
8 of the docs in a zip?

9 A. I should be able to, yeah.

10 MR. OLIVER: Nick, if it would be easier, I
11 believe Dr. Clark might have a folder with clean copies
12 of most of this, so -- but feel free if you want to send
13 your own zip file.

14 THE WITNESS: Yeah. I -- in that folder I
15 just opened, I haven't opened any of the files. But I
16 have exhibits 1005 through 1009, 2001 through 2007, and
17 exhibits 1014 through -- it looks like 1024. So...

18 BY MR. STEPHENS:

19 Q. Okay. And those are clean copies?

20 A. Yes.

21 Q. Okay. I would be fine if you want to
22 reference those. I think that will just be easier.

23 A. It will save some time. I don't expect we're
24 going to be pressed for time, but that's okay.

25 MR. STEPHENS: All right.

1 (Court reporter requested clarification.)

2 MR. STEPHENS: I'll drop them in right now if
3 you'd like to grab them.

4 BY MR. STEPHENS:

5 Q. Dr. Clark, I'd first like to refer to your
6 discussion of the Settimi reference in your declaration.

7 A. Yes.

8 Q. It's specifically paragraph 3.

9 A. Okay.

10 Q. And in the last sentence of paragraph 3, you
11 state, "Unlike the types of low-resolution databases
12 that Evenhaim discusses, Settimi's centralized
13 warehouse," quote, "'retain[s] clinically useful
14 information about the patient,'" end quote, "including,
15 for example," quote, "'dates of examination,
16 documentation, diagnosis, prescription, and lab test
17 results.'"

18 Did I read that correctly?

19 A. Yes.

20 Q. You cite paragraphs 38 and 40 from Settimi,
21 correct?

22 A. Yes.

23 Q. All right. So I'd like to take a look at
24 paragraph 39 in Settimi.

25 And let me know when you have that available.

1 A. Do we know which number exhibit Settimi is?

2 Q. Yes. It is Exhibit 1006.

3 A. I do not have that in this folder, it looks
4 like.

5 Q. I can drop it in the chat.

6 A. Yeah, let's do it that way. I don't want to
7 go searching on you.

8 MR. OLIVER: Sorry to interrupt. In that
9 folder, take a look at the second document.

10 THE WITNESS: That's 2003?

11 MR. OLIVER: Oh, no. There should be one
12 that's 1006.

13 THE WITNESS: 1006 is not in -- there's 2006
14 and 1016.

15 MR. OLIVER: Okay. Sorry. I -- it's in the
16 chat.

17 THE WITNESS: Okay. Let's do that. Make it
18 easier.

19 BY MR. STEPHENS:

20 Q. I'm going to turn to paragraph 39 in Settimi.

21 A. Yes, I recall.

22 Sorry, I'm having some technical difficulties.

23 Q. Take your time.

24 A. Yeah, the faster you try and type, the worse
25 it gets.

1 What I have is the patent, so I'm not sure
2 about paragraph 39. Is that -- oh, I see it. I've got
3 it. Never mind. 38.

4 Q. And by "the patent," you're referring to
5 what's -- to the Settini reference, right? I think it's
6 labeled U.S. 2007/0294111.

7 A. Yes, that's the one I downloaded.

8 Q. All right.

9 A. So I'm at paragraph 39.

10 Q. Yes.

11 All right. And about halfway down that
12 paragraph, you'll see there's a sentence that reads, "In
13 an exemplary embodiment of the present invention, the
14 following identifiers are removed or transformed in
15 order to create de-identified data that would be
16 classified under the HIPAA definition as fully
17 de-identified data."

18 Do you see that?

19 A. I do.

20 Q. And then Settini goes on to list the set of
21 identifiers that can be removed to create the fully
22 de-identified data, correct?

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

24 Q. Are you familiar with HIPAA's safe harbor
25 method of de-identification?

1 A. I've heard of it. I don't have it from
2 memory.

3 Q. What's your understanding of the safe harbor
4 method?

5 A. Safe harbor, as I understand it, is sort of a
6 minimum compliance standard.

7 Q. And so the safe harbor method, is it specified
8 in the HIPAA Privacy Rule?

9 A. I think it's specified multiple places in
10 HIPAA, or referenced, at least.

11 Q. Are you familiar with the HIPAA Privacy Rule?

12 A. I've read it, yes. Again, I didn't memorize
13 it.

14 Q. And does the HIPAA Privacy Rule provide for
15 different methods of de-identification?

16 A. I would assume that it contemplates it, but as
17 I said, I haven't memorized it.

18 Q. Based on your understanding of the safe harbor
19 method, why would a POSITA choose to de-identify data
20 according to the safe harbor method?

21 A. That would depend upon the requirements of the
22 system that were being implemented.

23 Q. And why might a POSITA choose the safe harbor
24 method as opposed to other methods?

25 A. That would have been a system requirement by

1 the system designers.

2 Q. Are there any specific advantages to the safe
3 harbor method that you're aware of?

4 A. Well, as I said, it's a minimum compliance
5 standard. So if you're concerned with perhaps liability
6 or something like that, you would -- some implementers
7 or designers might choose to comply with that. There
8 are other ways.

9 Q. But you agree that there are other ways of
10 doing de-identification that would comply with HIPAA,
11 correct?

12 A. I think there are lots of ways to do
13 de-identification in architect systems that comply with
14 HIPAA.

15 Q. And why would a POSITA choose to de-identify
16 data according to the safe harbor method as opposed to
17 those other methods that you have indicated?

18 A. As I said, that would have been a system
19 requirement by the designer.

20 Q. But are there any specific reasons that a
21 POSITA would choose the safe harbor method as opposed to
22 other methods?

23 A. I'm not sure the POSITA would be making the
24 choice unless that was the system designer. They might
25 actually be the implementer.

1 So the answer is I don't know. We're speaking
2 hypothetically right now.

3 Q. But in your experience, you're not able to
4 identify any particular reasons that a -- someone would
5 choose to use the safe harbor method as opposed to other
6 methods?

7 A. Actually, you asked me that question earlier,
8 and I gave you exactly such an example which was that,
9 if someone -- a designer was concerned with liability,
10 that a safe harbor implementation might be the way to
11 go.

12 Q. Okay. But you would agree that other methods
13 would also comply with HIPAA and therefore not yield
14 liability, correct?

15 A. There are lots of ways to comply with HIPAA.

16 Q. I'm just asking: What are the reasons that a
17 POSITA would choose the safe harbor method as opposed to
18 other methods?

19 A. I think I already answered that, Counselor.

20 Q. So turning, I guess, back to paragraph 39 in
21 Settimi, would a person of skill in the art understand
22 Settimi's description of fully de-identified data here
23 to mean data that's been de-identified according to the
24 safe harbor method?

25 A. No. It says pretty clearly -- and I didn't

1 cite to 39 for this reason -- that, for instance, in 40
2 that I did cite to -- where they talk about other
3 exemplary embodiments. So this is -- 39 is merely one
4 embodiment. There are lots of ways to do it.

5 Q. That wasn't my question.

6 I was asking -- or maybe -- maybe -- I just
7 want to be clear, and you may have answered it.

8 But is the method that's described in
9 paragraph 39 consistent with the safe harbor method of
10 de-identification in HIPAA?

11 A. I don't know. I haven't done that analysis.

12 Q. Would a person of skill in the art be familiar
13 with the safe harbor method?

14 A. Familiar with and memorizing all the
15 requirements are two different things. So, yeah, I
16 think someone said -- such as myself would know broadly
17 what it is, but you would have to go to the standard to
18 implement it specifically.

19 Q. Are there reasons that a person of skill in
20 the art would elect not to pursue the safe harbor method
21 and instead use another method of de-identification?

22 A. Well, again, as I said, it depends on how the
23 system is architected and what the systems are. If you
24 have trusted individuals who are entitled to see the
25 PII, then there might be different ways to implement

1 different systems if those people are involved because
2 they fall out -- I think they fall outside of the safe
3 harbor. I'd have to read it to make sure.

4 But the -- if you de-identify to that level,
5 then I would assume the presumption is that you don't
6 have such trusted people with access to the information.

7 Q. You're referring to people that would fall
8 outside of the safe harbor.

9 Can you explain what you mean by that?

10 A. Well, yeah. Can we just pull up the
11 requirements for safe harbor so that we can speak
12 specifically to this?

13 Q. Well, I'm asking, I guess, first, for you to
14 clarify your response there. You referred to people
15 outside of the safe harbor, and I just want to know what
16 you mean --

17 A. I'm not sure that they are outside of the safe
18 harbor. I'm going from memory.

19 But people who have access to the -- the PII
20 would not be accessing a database such as the one you
21 described necessarily.

22 Q. And what database do you believe I was
23 referring to at --

24 A. The one -- the one -- the one that's fully
25 de-identified, they would not have to necessarily access

1 because they have access to the PII. So the embodiment
2 of paragraph 39, they may or may not access. Again,
3 depending upon their own particular requirements.

4 Q. Sir, if you would like to reference -- I can
5 put this in the chat, but I believe you mentioned you
6 have it as well -- it's Exhibit 2006, which contains the
7 text of the HIPAA Privacy Rule, including the
8 requirements for de-identification according to the safe
9 harbor method.

10 A. Okay. I have it up.

11 Q. You have that, you said?

12 A. Yes.

13 Q. Okay. And under subsection (b)(2)(i), there
14 are a list of identifiers that would be removed
15 according to what we've been referring to as the safe
16 harbor method.

17 Do you see that?

18 A. I do.

19 Q. Do those identifiers correspond to the
20 identifiers listed in paragraph 39 of Settimi?

21 A. Let's have a look.

22 Yes. Maybe not all of them. I haven't
23 matched them one for one, but I see some of them.

24 Q. Okay. So based on your understanding, would a
25 POSITA have understood the method of de-identification

1 disclosed in paragraph 39 of Settimi to refer to the
2 safe harbor method?

3 A. Certainly for the ones that I can see, it
4 looks like they are lining up. But, again, it's --
5 paragraph 39 is just talking about a particular
6 embodiment. So I don't understand why we're arguing
7 about this.

8 Q. Now, one of the identifiers that would be
9 removed, according to the method described in
10 paragraph 39 of Settimi, are "geographic subdivisions
11 smaller than a state including street address, city,
12 county, precinct, zip code (down to the last three
13 digits)."

14 Correct?

15 A. That's what it says.

16 Q. So a searcher would be unable to search for
17 individuals in data that was de-identified as described
18 in this paragraph based on the smaller geographic
19 subdivisions, correct?

20 A. For this embodiment, that's correct.

21 Q. And that's because, in this embodiment, it
22 requires removal of more granular location subdivisions?

23 A. Well, that's what it says.

24 Q. Okay. Let's turn to the next paragraph,
25 paragraph 30. I'm sorry, paragraph 40.

1 A. I knew what you meant.

2 Q. And this paragraph refers to limited data sets
3 under HIPAA, correct?

4 A. That's what it says.

5 Q. Are you familiar with limited data sets and
6 HIPAA?

7 A. I don't have them memorized, but, I mean, I
8 can see that it's a different data set than the safe
9 harbor data set.

10 Q. What's your understanding of the difference
11 between a limited data set and the data set that's been
12 de-identified according to the safe harbor method?

13 A. Looks like they are taking more stuff out for
14 safe harbor, or at least according to this description
15 of it.

16 Q. So creation of a limited data set requires
17 removal of less information than the safe harbor method?

18 A. Let's see.

19 Yes. Because, here, the zip codes aren't
20 limited; the city and state are in there. So in the
21 safe harbor, they are taking out broader geographic
22 identifiers, and, here, they are leaving them in.

23 Q. Why would a -- why would one seek to create a
24 limited data set as opposed to de-identified information
25 according to the safe harbor method?

1 A. Because it provides higher resolution and less
2 information loss when you're de-identifying.

3 Information loss reduces the usefulness of the data.

4 Q. And the safe harbor method would yield more
5 information loss?

6 A. According to what I'm seeing here, yes.

7 Q. Is a limited data set considered protected
8 health information under HIPAA?

9 A. I don't know. It could be. I mean, I'd have
10 to look at the particular data set to see if it had PII
11 in it.

12 Q. What's your understanding of protected health
13 information in HIPAA?

14 A. Information that you're not allowed to
15 disclose except to individuals who are authorized to see
16 it.

17 Q. So HIPAA imposes restrictions on the
18 disclosure of protected health information; is that
19 correct?

20 A. Yes.

21 Q. And you are unaware whether a limited data set
22 is -- qualifies as protected health information?

23 A. I'm pretty sure I didn't say that, Counselor.
24 I said it would depend on the particular data
25 set. And I would have to look at it.

1 Q. What kind of things would you be looking at to
2 assess whether it qualified as protected health
3 information?

4 A. To see if it had PII in it.

5 Q. What are some examples of PII?

6 A. Names, Social Security numbers.

7 Q. And how would you make an assessment, then, of
8 a limited data set to determine whether it qualified as
9 protected health information?

10 A. See if the system was available to disclose
11 PII. I mean, that's -- they do that for HIPAA
12 evaluations all the time.

13 Q. So there would be instances, you believe, that
14 a limited data set could be protected health information
15 under HIPAA?

16 A. No, not necessarily. But it could
17 certainly -- if the system was not implemented properly,
18 it could certainly allow an attacker to determine PII.

19 Q. And there might be instances where, in your
20 view, protected health information -- I'm sorry, there
21 might be instances where limited data sets would not be
22 protected health information under HIPAA?

23 MR. OLIVER: Objection. Form.

24 THE WITNESS: Yes, I think you would have to
25 look at the individual case, but it's possible to

1 improperly implement pretty much any of these kinds of
2 systems, which is sort of the subject of the -- all the
3 patents and references we're talking about.

4 BY MR. STEPHENS:

5 Q. Let's refer to Exhibit 2006 again.

6 And specifically subsection (e), which is on
7 page 3 of the pdf.

8 Do you see that?

9 A. I'm getting it.

10 Okay. I'm looking at it.

11 Q. And this section refers to requirements for a
12 limited data set under HIPAA, correct?

13 A. Yes. In particular, it talks about covered
14 entities, which I refer to as trusted individuals.
15 People who have access to the PII.

16 Q. And in subsection (e)(2), it states, "A
17 limited data set is protected health information."

18 Correct?

19 A. That's what it says.

20 Q. Why would HIPAA classify limited data sets as
21 protected health information?

22 A. Because it might contain it; it might not.
23 Depends on the particular data set.

24 Q. Does HIPAA distinguish limited data sets from
25 de-identified information?

1 A. I don't know from memory. I'm sure that
2 there's some discussion of both as separate things. But
3 we could -- if you have something you want me to look
4 at, I'll look at it.

5 Q. Well, you offered opinions about limited data
6 sets and de-identified information, and you've also
7 offered opinions regarding HIPAA privacy rules.

8 So I'm asking: Based on your understanding,
9 is there a distinction between limited data sets and
10 de-identified information under HIPAA?

11 A. There can be is my answer. It depends on how
12 it's implemented.

13 Q. How what's implemented?

14 A. How the data sets are implemented. The
15 fields, the -- what, if any, de-identification is going
16 on.

17 Q. So your answer is that whether a limited data
18 set is de-identified information depends on the
19 implementation?

20 A. Whether -- it's a question of whether and to
21 what degree it's de-identified.

22 Q. Would a person of skill in the art have
23 understood that HIPAA imposes restrictions on a covered
24 entity's ability to disclose limited data sets?

25 A. Yes.

1 Q. And what kind of restrictions would those be?

2 A. You're not allowed to do it without the
3 permission of the subject.

4 Q. Who is the subject that you're referring to?

5 A. The patient.

6 Q. So disclosure of a limited data set would
7 require the authorization of a patient?

8 A. Depending upon what's in it.

9 Q. Are there any other mechanisms for a covered
10 entity to disclose a limited data set under HIPAA?

11 A. I'm sure there probably are.

12 Q. But none come to mind as you're sitting here
13 today?

14 A. I'm not sitting here having memorized the
15 HIPAA standard, no.

16 Q. You cited to Settimi's disclosure of limited
17 data sets, correct?

18 A. I'm sure that I did.

19 Q. And you contended that the disclosure of
20 limited data sets was relevant to the alleged
21 obviousness of the claims of the '641 patent, correct?

22 MR. OLIVER: Objection to form.

23 THE WITNESS: Again, if you want to point me
24 to a particular place in my declaration, I'll look. I
25 have not memorized it in its entirety, either.

1 BY MR. STEPHENS:

2 Q. Can you give me an example of a restriction
3 that HIPAA imposes on the disclosure of limited data
4 sets?

5 A. Yes. You are not allowed to disclose certain
6 information about patients.

7 Q. You would agree that there's information loss
8 in the creation of a limited data set, correct?

9 A. There can be. Again, it depends on how it's
10 implemented.

11 Q. How would you implement a system that created
12 a limited data set without information loss?

13 A. I'd encrypt the fields that I didn't want the
14 public to have access to.

15 Q. And that would, in your view, meet the
16 requirements of HIPAA's limited data sets?

17 A. It would be one way to do it. You could also
18 partition the database in two different data sets.
19 There are lots of engineering approaches to storing
20 information securely.

21 Q. There might be a lot of engineering
22 approaches, but I'm asking about regulatory compliance
23 and compliance with HIPAA.

24 Would all those approaches comply with HIPAA?

25 A. Not necessarily. You would have to check it

1 against the standard. But there are lots of
2 countermeasures that can be employed to de-identify that
3 don't necessarily reduce the resolution of the database.

4 Q. Creation of a limited data set under HIPAA
5 requires the removal of certain direct identifiers,
6 correct?

7 A. That's the way it's phrased, yes.

8 Q. And so by removing those identifiers, there is
9 information loss, correct?

10 A. Not necessarily. It depends on how they're
11 removed and whether they're retained.

12 Q. So I guess I'm a little confused by your
13 response because we -- I think we are in agreement that
14 a creation of a limited data set requires removal of the
15 direct identifiers specified in the HIPAA Privacy Rule,
16 correct?

17 A. That's what it says in the HIPAA Privacy Rule,
18 but it doesn't tell you exactly how to implement that.

19 Q. But then you, I believe, said in your last
20 response that those identifiers may be retained.

21 How do you remove the identifiers and yet
22 retain them is, I guess, what I'm trying to understand.

23 A. You can put them in a different data set. The
24 plain text can be removed. You could put a pointer in
25 in place of the plain text and control who has access to

1 the pointer. There are lots and lots of ways to
2 implement that in a compliant fashion.

3 Q. How do you know that the solution would be
4 compliant?

5 A. Because that would render the protected
6 information unavailable except to trusted individuals or
7 entities.

8 Q. Is that what the rule requires, just that that
9 information be unavailable?

10 A. Right. Has to be removed so that it's
11 unavailable.

12 Q. Are there any -- is there any text or
13 references that come to mind that support this -- the
14 way that you've described the ability to create a
15 limited data set?

16 A. I don't know. I have 30 years' experience in
17 secure database, so I'm willing to go out on a limb and
18 tell you there are lots of ways to implement systems in
19 a HIPAA-compliant fashion. And that's from direct
20 experience.

21 Q. The information that would be available in a
22 limited data set would have a lower resolution than the
23 original data, correct?

24 A. Potentially. I mean, not necessarily, but
25 potentially.

1 Q. So I -- you give these kind of answers that
2 are not entirely clear.

3 Can you give me an example of how the limited
4 data set would be -- would not have a lower resolution
5 than the original data set in terms of the information
6 that is actually available from the limited data set?

7 A. Sure.

8 If everybody in the study is from a single
9 state and you remove the state, then there's no
10 information loss because everybody is from one state.

11 So the reason there's -- you would like to
12 come up with absolute definitions in order to make your
13 arguments. Unfortunately, there aren't any. HIPAA is a
14 guideline. It's a standard, and there are lots and lots
15 of engineering approaches to implement HIPAA-compliant
16 systems. And you're going to have to accept that.

17 Q. I'm just asking about the requirements under
18 HIPAA, your understanding of it.

19 A. And I understand what you're asking. I'm
20 giving you answers, and you're accusing me of being
21 unclear, and I'm being anything but unclear.

22 I'm just telling you there are lots of ways to
23 implement these systems. And Settimi, the reference
24 we're talking about, tells you that there are lots of
25 alternative exemplary embodiments that could be

1 compliant.

2 Q. In the example that you just gave, you
3 referred to removing information about the state of the
4 patient, correct?

5 A. Yeah, that's one broad example where you would
6 not have information loss by removing a field.

7 Q. But in that example, there is information loss
8 because no longer is the state associated with the
9 individual, correct?

10 A. But if they all came from the same state, then
11 there would be no information loss in dropping the
12 state.

13 Q. Okay. I'd like to next turn to Settimi's
14 discussion of encoded patient identifiers, which you
15 refer to in paragraphs 5 and 7 of your declaration.

16 And if I use the term "EPID," will you
17 understand that I'm referring to an encoded patient
18 identifier in Settimi?

19 A. Yes.

20 Q. So I'd like to turn to paragraph 41 of
21 Settimi, please.

22 Do you see that?

23 A. I do.

24 Q. And this paragraph describes how an EPID is
25 created by a patient care provider, or, for short, PCP,

1 based on the patient identifier 304 and the password.

2 Do you see that disclosure?

3 A. Yes.

4 Q. And Settimi explains that, quote, "Password
5 string 312 is known only to the PCP and is required in
6 order to decode the EPID 308 into a PID 304."

7 Do you see that?

8 A. That's what it says.

9 Q. Why is it important that the password string
10 be known only to the PCP?

11 A. Because otherwise they would be able to decode
12 the PID.

13 Q. And the PID is, just for the record, patient
14 identifier, correct?

15 A. Yes.

16 Q. You said it would be important that the
17 password be known only to the PCP because otherwise they
18 would be able to decode the PID?

19 A. In this embodiment, yes.

20 Q. And that would be to -- they would be able to
21 decode the EPID, correct?

22 A. Depending on how it's implemented. But, I
23 mean, this -- the way it's suggested is that you would
24 be able to use symmetric techniques to decode it if you
25 had the password.

1 Q. So if a password were leaked to an
2 unauthorized third party, for example, and that third
3 party came into possession of an EPID, they could use
4 the password to re-identify the patient?

5 A. Potentially. I mean, not necessarily, but
6 potentially.

7 Q. And so the PCP would want to keep the password
8 in confidence, correct?

9 A. In this embodiment, yes.

10 Q. If a -- if an entity lacked the password, then
11 they would be unable to create the EPID, correct?

12 MR. OLIVER: Objection. Form. Foundation.

13 THE WITNESS: Yeah. In this embodiment, which
14 describes a symmetric two-fish algorithm, then you would
15 require the key, the password, in order to encrypt and
16 decrypt the PID.

17 BY MR. STEPHENS:

18 Q. So the password is necessary in order to
19 encrypt the PID to create the EPID, correct?

20 A. In this embodiment, yes.

21 Q. And, likewise, the PID itself is required to
22 create the EPID, correct?

23 A. And the algorithm.

24 Q. So if you lack either the password or the PID,
25 you'd be unable to create the EPID, correct?

1 A. Or the alg- -- the encryption algorithm. You
2 would be unable to either encrypt or decrypt.

3 Q. In paragraph 38, Settimi notes -- this is a
4 long paragraph, so I'm looking at it, but the left
5 column on page 5 of Settimi.

6 About halfway down that paragraph, it says,
7 "Other unique identifying numbers, characteristics, and
8 codes assigned by the PCP or by the EMR system for
9 administrative purposes, including a patient identifier
10 (PID) 304."

11 Do you see that?

12 A. Yeah, I do.

13 Q. And so the EMR system is a system that's
14 maintained by the PCP, correct?

15 A. In this example, yes.

16 Q. And the patient identifier (PID) 304 is an
17 identifier that's assigned by the PCP or the EMR system,
18 correct?

19 A. In this example, yes. But it doesn't say
20 whether it might be calculated or not, but it says
21 they're assigned.

22 Q. And the PID uniquely identifies an individual
23 in the EMR system, correct?

24 A. In that particular system, in this example,
25 yes.

1 Q. And the PID would -- is the PID known to
2 entities other than the PCP?

3 A. I don't know. It depends.

4 Q. In this embodiment, though, this says that a
5 PCP or the EMR system assigns the PID to the patient
6 record, correct?

7 A. That's what it says.

8 Q. You mentioned earlier that the password can be
9 used to decrypt the EPID to recover the PID; is that
10 right?

11 A. I'm not sure that's the same embodiment, but,
12 I mean, that's certainly one way to do it.

13 Q. So the -- is the PCP, then, able to attain the
14 identity of the patient from the EPID?

15 A. I would think it would be implemented in such
16 a way, but that information would have to be protected
17 separately. And this is what we were discussing
18 earlier.

19 Q. What information would need to be protected
20 separately?

21 A. Well, they would -- as a trusted individual,
22 the PCP would probably want to be able to look up the
23 PID and find out who it was and the other information
24 about them. So I would expect that information to be
25 retained somewhere.

1 Q. And, again, I think you mentioned this
2 earlier. When you say "trusted individual," you're --
3 does that mean a covered entity under HIPAA?

4 A. Yes. I mean, that's what HIPAA calls them.
5 In general, you have trusted individuals in system
6 security, and those would include people like
7 administrators and, in this case, doctors and their -- I
8 think their subcontractors or whatever.

9 But, yes, they are basically -- they call them
10 "covered entities."

11 Q. So the PCP is able to use its password to
12 re-identify the patient from the EPID, correct?

13 A. Again, it depends on how it's implemented. I
14 think you're miss -- you may be mixing embodiments, but
15 from the disclosure, you could certainly do it that way.

16 Q. I mean, could you do it that way, or does
17 Settimi disclose that you can -- that you do it that
18 way?

19 A. From my reading of it, it's providing options
20 in different embodiments. So, you know, a person of
21 skill would know to combine those along with others.

22 Q. Now, Settimi -- strike that.

23 Settimi discloses techniques for the PCPs to
24 re-identify patients from the EPIDs, correct?

25 MR. OLIVER: Objection --

1 THE WITNESS: In the paragraph we described,
2 it says this is how you get access to the PID. So then
3 if it wanted to re-identify -- if a system objective was
4 to re-identify, then it would have to store that
5 identifying information for the PID somewhere securely.

6 BY MR. STEPHENS:

7 Q. Is the PID identifying information for an
8 individual?

9 A. Depends on how it's implemented.

10 Q. So the PID is a patient identifier, correct?

11 A. That's what it is.

12 Q. And it therefore uniquely identifies the
13 patient in the PCP system, correct?

14 A. No, in the EMR system. That particular EMR
15 system.

16 Q. That particular EMR system being the
17 particular EMR system for a PCP?

18 A. That's the way I understand it from that
19 paragraph, yes.

20 Q. What does re-identification mean to you in
21 Settimi?

22 A. That would be the ability to identify the
23 patient specifically from whatever the EPID is.

24 Q. Are there -- strike that.

25 Let's turn to paragraph 47, please. That's

1 Settimi.

2 Do you see that?

3 A. Yes.

4 Q. And, here, Settimi explains that a user --
5 quote, "A user may search for one or more patient
6 records within EMR by invoking a 'find' dialogue or
7 search function."

8 Correct?

9 A. In certain embodiments, as it says at the
10 start of the paragraph.

11 Q. Yes.

12 And then, "The user may search by the EPID,
13 for example, and enter or select an EPID number to
14 activate a search," correct?

15 A. That's what it says.

16 Q. And what's the EMR, again, that Settimi refers
17 to in this paragraph?

18 A. That's the system being used by the PCP.

19 Q. Electronic medical records system?

20 A. Yes.

21 Q. Is the EMR shown in Figure 2 of Settimi?

22 A. There are several of them shown in Figure 2.

23 Q. Where are they shown in Figure 2?

24 A. They are shown as front-ending the data
25 warehouse.

1 Q. But these -- the EMRs are shown within the
2 PCP, the boundaries of the PCPs, correct?

3 A. Yes. For this particular figure, yes.

4 Q. So the EMRs here are distinct from the data
5 warehouse system, correct?

6 A. Not necessarily, but you could -- I mean,
7 they're listed as separate components for this
8 embodiment.

9 Q. So as shown here, the EMRs are distinct from
10 the central data warehouse system, correct?

11 A. They are separate boxes.

12 Q. What does that -- how would a POSITA have
13 understood that, seeing that there were separate boxes?

14 A. Separate components, how they are particularly
15 deployed, you know, can vary. This is a particular
16 embodiment that has multiple PCPs feeding the data
17 warehouse.

18 Q. And would a POSITA understand that the -- each
19 PCP is associated with a respective EMR system?

20 A. For this embodiment, it only shows one, but,
21 again, these are boxes that are logical components.
22 This is not a hardware implementation.

23 Q. So going back to paragraph 47, again, Settimi
24 describes how the patient records can be searched within
25 an EMR by the EPID, correct?

1 A. In certain embodiments, according to
2 paragraph 47, that's how you can search within an EMR.

3 MR. STEPHENS: All right. We've been going
4 for a bit over an hour. Why don't we take a break.

5 Would -- I'd like a little bit more time for
6 this one. Would 15 minutes work for you, Dr. Clark?

7 THE WITNESS: Yeah, I'll plan to be back at
8 11:30.

9 MR. STEPHENS: Okay.
10 Is that okay, Justin?

11 MR. OLIVER: Sure.

12 MR. STEPHENS: All right. Thanks. Off the
13 record.

14 (Recess: 11:11 a.m. to 11:34 a.m.)

15 BY MR. STEPHENS:

16 Q. So I'd like to refer to paragraph 12 of your
17 declaration.

18 A. Okay.

19 Q. And in this paragraph, you refer to the
20 concept of a business associate under HIPAA, correct?

21 A. Yes.

22 Q. What is a business associate?

23 A. It's a trusted entity that is in some way
24 related to the provider in a business way.

25 Q. And a business associate is defined under the

1 HIPAA rules, correct?

2 A. Yeah. I think they have examples. I'm not
3 sure it's exhaustive.

4 Q. You state in this paragraph that -- and
5 specifically, this is the sixth line down --
6 "Specifically, a covered entity can contract out certain
7 functions to business associates so that those entities
8 can handle protected healthcare data without it being a
9 HIPAA violation."

10 Correct?

11 A. Yes.

12 Q. A business associate can therefore handle
13 protected health information under HIPAA from a covered
14 entity with which it has a business associate agreement;
15 is that right?

16 A. Yes, sir.

17 MR. OLIVER: Objection. Well...

18 BY MR. STEPHENS:

19 Q. When there's a BAA in place -- and I'll state
20 BAA is short for business associate agreement.

21 Do you understand that?

22 A. Yes.

23 Q. When a BAA is in place between a covered
24 entity and another entity, there would be no need to
25 de-identify patient data records before disclosing those

1 records to the business associate to comply with HIPAA,
2 correct?

3 A. Well, not necessarily. I mean, there may be
4 reasons that you don't want to disclose everything to a
5 business associate. Again, it depends on the system and
6 what you're sending and what their role is.

7 From a security perspective, you would
8 generally minimize only to the stuff that they need the
9 data that they would receive. I mean, that's sort of a
10 standard concept in security.

11 Q. But under HIPAA, a business associate
12 agreement would allow a covered entity to disclose
13 protected health information to its business associate,
14 correct?

15 A. It's possible, sure. I mean, it depends --
16 depends on the particular situation.

17 Q. And, conversely, a business associate
18 agreement would not be needed for a covered entity to
19 disclose de-identified information to a third party,
20 correct?

21 A. Yeah, not necessarily correct. It depends.
22 If -- we had our discussion about limited data sets and
23 safe harbor and everything else. Probably, if you were
24 disclosing safe harbor data, that would be correct. But
25 not necessarily the case.

1 Q. So if a covered entity de-identified its
2 patient data sets according to the safe harbor method, a
3 business associate agreement would not be necessary in
4 that instance for it to disclose the de-identified
5 information to a third party?

6 MR. OLIVER: Objection. Form.

7 THE WITNESS: Yeah. I mean, that's possible,
8 I mean, if it's fully de-identified. There may be other
9 reasons to have an agreement in place.

10 BY MR. STEPHENS:

11 Q. But fully de-identified data would not -- the
12 disclosure of fully de-identified data would not require
13 a business associate agreement, correct?

14 A. Not under HIPAA, no.

15 Q. Would the disclosure of a limited data set
16 under HIPAA require a business associate agreement?

17 A. Maybe; maybe not. Again, it depends.

18 Q. Are you aware of any provisions in HIPAA that
19 would require a business associate agreement for the
20 disclosure of limited data sets?

21 A. Yeah. There would be reasons to do that if
22 you were worried about liability in some way, if you
23 were not fully safe harbor. So the answer is it's
24 possible that you would want to have such an agreement.
25 Contracting agreements are routinely done for -- between

1 businesses, independent of HIPAA.

2 Q. Yeah. And to be clear, my questions are
3 pertaining specifically to business associate agreements
4 under HIPAA.

5 So with that in mind, would a business
6 associate agreement be necessary to disclose a limited
7 data set to a third party under HIPAA?

8 A. Maybe; maybe not. It depends on what else
9 they have access to. I don't know. I would have to
10 look at a specific example.

11 Q. Would your assessment turn on the specific
12 provisions regarding limited data sets in HIPAA?

13 A. No, it would depend upon the particular
14 situation and what the business associate was doing.

15 Q. So it might be necessary, in some cases, for a
16 business associate agreement to be in place for the
17 disclosure of limited data sets?

18 A. I can imagine it would be possible, yes.

19 Q. I'm not asking whether it would be possible.
20 Would it be necessary, under HIPAA, for the
21 disclosure of a limited data set to have a business
22 associate agreement?

23 A. I appreciate the response, Counselor.

24 By "possible," I mean it may be necessary to
25 do so from a business perspective. So it's possible

1 that that may be a requirement.

2 Q. Where would you look up to see if that were a
3 requirement?

4 A. I think I've already answered that. It would
5 depend upon the particular situation and the
6 relationship between the trusted party and the business
7 associate.

8 Q. All right. Can you explain what you mean by
9 "it would depend on the particular situation and the
10 relationship between the trusted party and the business
11 associate"?

12 A. As I said, it would depend upon what else they
13 might have access to and whether there was a security
14 risk or any other kind of risk that would require you to
15 have such an agreement in place.

16 Q. So there might be instances, is what I believe
17 you're saying, in which a business associate agreement
18 would be necessary for the disclosure of limited data
19 sets under HIPAA; is that correct?

20 A. As I said, it's possible, depending upon the
21 relationship, that I might have that as a requirement
22 from a business perspective.

23 Q. Again, my question is -- I'm not asking about
24 possibilities.

25 I'm asking: As a matter of complying with

1 HIPAA, is it necessary to have a business associate
2 agreement in place for the disclosure of limited data
3 sets?

4 A. It would depend -- I'll say it again -- on
5 what that business associate has access to as to whether
6 or not you would need the agreement.

7 Q. Would a -- would a central data warehouse that
8 stored only de-identified information -- let's say fully
9 de-identified information -- need a business associate
10 agreement to disclose that information to a third party?

11 MR. OLIVER: Objection --

12 THE WITNESS: It shouldn't -- it shouldn't is
13 the short answer. So in general, I would say no.

14 But, again, it depends on how the particular
15 system is architected. But in general, the purpose of
16 having the de-identified database in compliance with
17 HIPAA is so that it can be disclosed.

18 BY MR. STEPHENS:

19 Q. And with respect to limited data sets, would a
20 data warehouse that stored limited data sets need a
21 business associate agreement for the disclosure of those
22 limited data sets to third parties?

23 A. Well, since it's your time, I'll answer this
24 for the third or fourth or fifth time.

25 But the answer is it depends upon what else

1 that business associate had access to and what it was
2 disclosing. So the particulars of that situation
3 matter.

4 Q. Are there any other types of agreements that
5 would be necessary for the disclosure of a limited data
6 set under HIPAA?

7 A. It's possible. It depends upon the
8 particulars of the situation.

9 Q. Again, you've said -- you've said a number of
10 times that it depends on the particulars of the
11 situation. So I'm gathering that you have something in
12 mind as to, you know, what you would be considering to
13 assess whether the business associate agreement was
14 necessary.

15 What particulars are there? Can you give some
16 concrete examples?

17 A. No. I've given you my answer because all the
18 systems are different. It depends upon the particulars
19 of the relationship, the functions, the architecture of
20 the system. So there's not a one-size-fits-all answer.
21 So the answer is what it is.

22 Q. Now, as I understand your declaration, I --
23 you've contended that business associate agreements
24 could be used in the system of the Evenhaim/Settimi
25 combination; is that correct?

1 A. Absolutely.

2 Q. So I'm trying to understand how this would
3 work.

4 There's a number of different entities in the
5 system, correct?

6 A. Yes.

7 Q. And those could include the data aggregator,
8 correct?

9 A. Yes.

10 Q. And it would include a centralized data
11 warehouse as described in Settimi; is that correct?

12 A. That's the back-end system, yes.

13 Q. And that data warehouse would -- as I
14 understand it, would pull information from -- or receive
15 information from data source entities or PCPs. Is that
16 correct?

17 A. Through the aggregator.

18 Q. The data warehouse would receive the
19 de-identified information from the PCPs through the
20 aggregator?

21 A. Yes.

22 Q. Can you point to where that's described in
23 either Settimi or Evenhaim?

24 A. I can reference my declarations, if you wish.
25 We discussed that at some length last time that you

1 would use the data warehouse of Settimi to receive
2 queries and such and data through the aggregator.

3 Q. Do you have your first declaration available,
4 Exhibit 1003?

5 A. No.

6 Q. I'll put it in the chat.

7 All right. It should be up there.

8 A. The deposition document?

9 Q. I believe it's -- this is your declaration,
10 the first declaration submitted in this proceeding,
11 Exhibit 1003.

12 A. Okay. It says, "Deposition Document." I'm
13 asking if that's what you just put up there. If that's
14 the case, I'll download it.

15 MR. STEPHENS: Justin or Tamara, do you see in
16 the chat, does it say, "Deposition Document"? To me, it
17 says, "Exhibit 1003 - Clark First Declaration."

18 MR. OLIVER: Just for clarity, there's a zip
19 file that's called "Deposition."

20 MR. STEPHENS: Oh. Maybe scroll down in the
21 chat.

22 THE WITNESS: Oh, I found it. Yeah. Got it.
23 BY MR. STEPHENS:

24 Q. Okay. And my question here is simply -- you
25 mentioned that the -- in the Evenhaim/Settimi

1 combination, the data warehouse would receive
2 de-identified information from the data source entities
3 through the data aggregator.

4 And it would be helpful if you could point to
5 me where in your declaration you describe that -- that
6 functionality of this combination.

7 A. I mean, I'm going to have to go through the
8 whole thing. I mean, the combination's concerned with
9 queries, but it was also possible that the aggregator
10 could populate or update information in that warehouse
11 as well.

12 So I don't know if I explicitly said that or
13 not, but it's certainly possible that you could do that,
14 if that's helpful. If you want me -- if you would like
15 me to read the entire declaration, I can do so, but that
16 seems kind of wasteful.

17 Q. It may not be necessary.

18 Just so we're on the same page, could you
19 describe in this combination the dataflow between the
20 data source entities, the warehouse, and the data
21 aggregator?

22 A. So if you go to paragraph 39 of the first
23 declaration, it describes the interconnection of
24 the aggregator and the back-end system on it.

25 Q. My understanding is this paragraph pertains to

1 your first obviousness crown, which was based on
2 Evenhaim alone.

3 So my question is actually in the combination
4 of Evenhaim and Settimi. Could you describe the
5 dataflow between the data source entities, the
6 warehouse, and aggregator?

7 A. Yes.

8 The dataflow would go to the data warehouse as
9 described in paragraph 39. From there, the aggregator.
10 It's interconnected.

11 Q. And what would go to the data warehouse as
12 described in paragraph 39?

13 A. Generally, queries. And as we described and
14 discussed ad nauseam, the Evenhaim allows for encrypted
15 tokens to do the queries.

16 Q. So in the combination, the data warehouse is
17 importing de-identified information from the data source
18 entities; is that correct?

19 A. That's the origination site. The data path
20 could or could not go through the aggregator to do that
21 in terms of implementation. But, yes.

22 Q. So we've got these different entities in the
23 combination, including the data aggregator, the central
24 data warehouse, and the data source entities, correct?

25 A. Yes, they are all interconnected.

1 Q. Okay. Would the data source entities be
2 covered entities under HIPAA?

3 A. I would expect them to be.

4 Q. And would the data -- strike that.

5 Referring, again, back to paragraph 15 in your
6 second declaration, you've indicated that business
7 associate agreements could be used in the Settimi or
8 Evenhaim/Settimi combination, correct?

9 A. Yes.

10 Q. So I'm trying to understand specifically how
11 this would work.

12 Would the -- would the data aggregator in this
13 combination have a business associate agreement?

14 A. It certainly could. You -- this is a
15 responsive declaration, and you raised an objection to
16 the fact that the aggregator, if there was a bad actor
17 on the aggregator, could get in access to PII.

18 And if that was a realistic risk, depending
19 upon the implementation, a CBA could be used to address
20 that, and then there would be no HIPAA violation, as you
21 asserted in the declaration I was responding to.

22 Q. So the BAA, in your view, would avoid the
23 HIPAA violation that would otherwise occur?

24 A. It would not necessarily occur, but to the
25 extent that was a risk, you could use a CBA to avoid a

1 HIPAA violation.

2 Q. When you say "CBA," are you referring to a
3 business associate agreement?

4 A. Yes, covered -- yeah. We have an acronym
5 overload. Yes.

6 Q. Okay. Are the -- would the data warehouse in
7 the combination, as you've described it in paragraph 12
8 of your second declaration, have a business associate
9 agreement?

10 A. Again, it would depend -- I would expect it to
11 be a goal to not have it. But to the extent, depending
12 upon the way the system is architected, it might need
13 one to prevent a bad actor from disclosing PII.

14 Q. Why would it be a goal to not need to have a
15 business associate agreement?

16 A. Because you would like to have the database
17 publicly accessible or accessible generally without risk
18 of HIPAA violation. But it's not necessarily the --
19 it's not necessary that that be the case because of the
20 business agreements that can be employed to avoid HIPAA
21 violations.

22 Q. Are there any downsides to employing the
23 business associate agreement?

24 A. I don't know without a specific example.

25 Q. Well, I'll rephrase the question.

1 Why would it be preferred to use a -- to be
2 able to disclose the de-identified information without a
3 business associate agreement?

4 A. Well, as I described earlier, it is a goal of
5 any secure system, particularly when you're trying to
6 secure data, to employ what's called least privilege.
7 So, ideally, you would minimize the access.

8 And if I were designing the system, I would
9 probably try to minimize access to sensitive
10 information, particularly on that particular component,
11 so that you could make it more generally available and
12 obviate the need for an agreement -- such an agreement.
13 But if you needed it, you could employ it.

14 Q. And who would the business associate
15 agreement -- what entities would the business associate
16 agreement be between in this combination?

17 A. It could be any number. You have the
18 actors -- it depends on who's administering which
19 systems. So you've got the provider, you've got the
20 aggregator, and you've got the data warehouse, all of
21 whom are eligible for such an agreement.

22 Q. So there could be a business associate
23 agreement between the aggregator and the data warehouse?

24 A. If they needed it.

25 Q. And in that case, one of those entities would

1 be a covered entity, correct?

2 A. In theory. I mean, it's -- again, you can
3 comply with HIPAA through the use of the agreements.
4 That was the purpose of the statement in responding to
5 your assertion in your declaration. This is a reply.

6 Q. Well, I'm -- I'm asking about -- you did
7 submit this reply declaration, and I'm trying to
8 understand the opinions that you put in it.

9 A. All right. I'll make it easy.

10 My opinion is that, since you said it was a
11 HIPAA violation if they could access PII, I said, no,
12 according to HIPAA, you can have agreements, business
13 agreements, in place so that it's not a HIPAA violation.

14 That's the assertion, and I stand by it.

15 Q. Wouldn't you agree that the contracting
16 parties in a -- for a business associate agreement -- at
17 least one of those parties must be a covered entity
18 under HIPAA?

19 A. That's the way HIPAA is designed, yes.

20 Q. And so if there were a business associate
21 agreement in place between the data aggregator and the
22 warehouse, one of those parties would be a covered
23 entity, correct?

24 A. Yes. Or they could have an agreement with the
25 provider. I mean, there's -- the agreements are

1 intended to avoid HIPAA violations.

2 Q. So, you know, in the -- in this scenario that
3 you've described in paragraph 12 where there would be
4 business associate agreements in place, which of the
5 entities would be a covered entity?

6 A. The provider.

7 Q. Any other entities?

8 A. Again, we'd have to look at a specific example
9 of who is doing what. I mean, it's possible that the
10 person who owns the aggregator and administers that is
11 covered. It's -- I mean, it's not ruled out by the
12 reference by any means.

13 Q. If the provider were a covered entity and they
14 are disclosing fully de-identified data sets, why would
15 they use a business associate agreement with the data
16 warehouse?

17 A. As I said, there are business reasons, to the
18 extent they have access to information or could obtain
19 PII, that they would put those in place.

20 Q. But it wouldn't be necessary to comply with
21 HIPAA, correct?

22 A. If they are not worried about a HIPAA
23 violation, then it would not be necessary under HIPAA to
24 have such an agreement. That is correct.

25 Q. And if the HIPAA business associate agreement

1 were in place, it would not be -- let's say between the
2 data warehouse and the provider, it would not be
3 necessary for the provider to de-identify the patient
4 data before disclosing it to the warehouse, correct?

5 A. Not necessarily. Again, there are different
6 levels of de-identification, as we've described, and so
7 there may be reasons to have the agreements in place.

8 Q. Okay. Two levels, then, as examples.

9 First, the safe harbor method, there would
10 be -- let's consider information that's disclosed by the
11 provider to the data warehouse that's been de-identified
12 according to the safe harbor method. There would be no
13 need for a business associate agreement for disclosure
14 of that data, correct?

15 A. Not under HIPAA, but there may be other
16 reasons to do it, so -- as we've discussed ad nauseam.

17 Q. And you haven't identified any of those other
18 reasons in your declaration, correct?

19 A. Well, we're discussing them here now, and one
20 of the other reasons would be some other liability for a
21 disclosure. And, again, it would depend upon the
22 particular system and the functions of the associate.

23 Q. And let's consider data that's been generated
24 according to the limited data set techniques in HIPAA.

25 In that case, there would be no need for a

1 business associate agreement for disclosure of the
2 limited data sets to the data warehouse, correct?

3 A. No, not necessarily correct. We've already
4 discussed that.

5 Q. All right. Let's turn, then, to paragraph 23
6 of your declaration, the second declaration.

7 And the last sentence on page 17 -- well, I
8 guess, the third line, starting on the third line in
9 paragraph 23, you state, "Landi explicitly states that
10 its design presents," quote "'no HIPAA issues,'"
11 unquote, "and that its goal is HIPAA compliance."

12 Do you see that?

13 A. Yes.

14 Q. When you referred to HIPAA compliance here,
15 are you referring to compliance with the HIPAA Privacy
16 Rule?

17 A. I'm talking about the standard in general,
18 which allows the use of agreements, et cetera. That's
19 why it says, "(e.g., using business associates)."

20 Q. But one aspect of HIPAA compliance, at least,
21 would include compliance with the HIPAA Privacy Rule,
22 correct?

23 A. Not necessarily. It says there are options
24 under HIPAA that would make Landi's design not violate
25 HIPAA as you asserted.

1 Q. So your -- as you read Landi, then, Landi may
2 not be referring to -- its goal may not be compliance
3 with the HIPAA Privacy Rule?

4 MR. OLIVER: Objection. Form. Foundation.

5 THE WITNESS: Yeah. I don't even understand
6 why you would say that, Counselor. I mean, the
7 paragraph is very clear. Its design presents no HIPAA
8 issue -- issues, and its goal is HIPAA compliance.

9 That's what it says. I mean, it doesn't say
10 specifically "the Privacy Rule," though that -- you
11 know, that would be a good thing. But you could also
12 use business associates, which is what it also says.

13 I mean, the paragraph is pretty clear.

14 BY MR. STEPHENS:

15 Q. Well, I asked what I thought was a pretty
16 straightforward question.

17 You referred to Landi's goal being HIPAA
18 compliance, correct?

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

20 Q. And I asked that -- is this goal -- does that
21 include compliance with the HIPAA Privacy Rule. And you
22 stated and replied, "Not necessarily."

23 Is that your --

24 A. My answer is there may be other mechanisms
25 within HIPAA, like business associates, that allow

1 compliance beyond with just the privacy.

2 Q. Okay. And I'm not referring to business
3 associates.

4 My question pertains to your characterization
5 of Landi here. You state, "Landi's goal" --

6 Excuse me. I'm asking a question.

7 "Landi's goal is HIPAA compliance."

8 Does that include compliance with the HIPAA
9 Privacy Rule?

10 A. That is a first objective.

11 And I'd appreciate -- actually, I don't
12 appreciate you cherry-picking phrases out of a paragraph
13 when the paragraph stands on its own. And it says its
14 goal is HIPAA compliance.

15 And, sure, that would include the Privacy
16 Rule. To the extent that may or may not be possible,
17 you have business associate agreements.

18 Is that a good enough answer, or do you want
19 to parse -- maybe there's one word in there. I mean, I
20 don't appreciate that, Counselor. That's not cool.

21 Q. So just to be clear, Landi's goal of HIPAA
22 compliance would include compliance with the HIPAA
23 Privacy Rule?

24 A. I would think they would want to comply with
25 the HIPAA Privacy Rule, but to the extent that that

1 wasn't possible, they could use business associate
2 agreements and maintain HIPAA compliance, which is the
3 goal.

4 Q. Why would Landi want to achieve HIPAA
5 compliance?

6 A. Sort of the purpose of the reference, don't
7 you think?

8 Q. Would HIPAA compliance be an important
9 consideration to a POSITA?

10 A. If I was implementing a system that's covered
11 by HIPAA, yes.

12 Q. And in general, why would a -- why would --
13 why would you seek to design a system to be HIPAA
14 compliant?

15 A. Because it's managing protected data at some
16 level.

17 Q. Would a system that's HIPAA compliant be more
18 likely to attain industry induction than one that were
19 not compliant?

20 A. I -- I would think that that would be a system
21 requirement, and I have seen HIPAA certifications
22 offered by third parties. So I would think that would
23 be helpful for your sales efforts, yes.

24 Q. Now, in paragraph 19 of your declaration, you
25 have a paragraph pertaining to the Dick reference.

1 Do you see that?

2 A. Yes.

3 Q. And you state here that, "While Dick
4 acknowledges HIPAA restrictions and the benefits of
5 de-identification, Dick generally 'contemplates'
6 'methods and processes' for the same."

7 Do you see that?

8 A. Yes.

9 Q. So was Dick also concerned with HIPAA
10 compliance?

11 A. Yes.

12 Q. Given that one of Dick's goals was HIPAA
13 compliance, would a POSITA be motivated to implement
14 features in Dick's system that were not HIPAA compliant?

15 A. That wouldn't make sense to me. But, again,
16 as we've discussed, there are lots of ways to achieve
17 HIPAA compliance which are not specific to the Privacy
18 Rule alone.

19 Q. So implementing Dick's system to include
20 features that are not HIPAA compliant would be contrary
21 to Dick's goal; is that right?

22 A. I think that Dick generally contemplates, as I
23 said, methods and processes for HIPAA compliance, but it
24 doesn't describe specific de-identification methods or
25 technical mechanisms for doing so.

1 Q. Now, a couple places in your declaration,
2 paragraphs 20 and 23, you've referred to Landi's
3 encrypted IDs, so I'd like to ask some questions about
4 those.

5 A. Mm-hmm.

6 Q. Do you have the Landi reference available?

7 A. I do. I'd have to find it.

8 Q. This is Exhibit 1008.

9 A. Okay. Got it.

10 Q. Let's turn to column 5, lines 7 through 19, of
11 Landi.

12 A. Okay.

13 Q. And this section describes how Landi's
14 encrypted IDs are created; is that correct?

15 A. No. If you look again at the bottom of
16 column 4, it says this is one exemplary embodiment that
17 describes the public key (RSA) implementation of that.
18 So this is one example.

19 Q. This is one example of how Landi creates an
20 encrypted ID; is that correct?

21 A. One example of how you could create an
22 encrypted ID using public key rather than symmetric key
23 methods.

24 Q. So Landi explains here that the healthcare
25 entity can use a key to encrypt, quote, "one or more

1 items of patient identifying information contained in
2 the respective patient medical records owned/managed by
3 the healthcare entity to thereby generate an encrypted
4 ID for each subject patient."

5 Correct?

6 A. That's what it says.

7 Q. So Landi's encrypted ID is derived from
8 information about the individual, correct?

9 A. Yes.

10 Q. Now, let's look at column 6, line -- the
11 paragraph starting at line 56.

12 Take a moment to read it, if you'd like.

13 A. Yes.

14 Q. And this paragraph describes
15 re-identification, correct?

16 A. It describes another embodiment that allows
17 re-identification, yes.

18 Q. Claim 3. Let's look at Claim 3 of Landi.
19 This is in column 15 at line 18.

20 And this reads, "The method of Claim 1,
21 further comprising securely maintaining a decryption
22 key, which can be accessed by an authorized entity to
23 decrypt the encrypted ID in the de-identified data
24 record to re-identify the patient."

25 Correct?

1 A. Yes. Referencing the embodiment that we
2 previously discussed.

3 Q. So that encrypted ID provides a means for -- a
4 means to allow de-identified information to be
5 re-identified to the healthcare entity?

6 A. Depending upon the embodiment, yes.

7 Q. And the healthcare entity in Landi would be a
8 covered entity under HIPAA, correct?

9 A. Maybe. I mean, again, it depends on the
10 particular embodiment.

11 Q. Now, in Figure 1 of Landi, there is a box in
12 the bottom left labeled "30."

13 Let me know if you see that.

14 A. Okay. I see Figure 1.

15 Q. And I'm looking at the -- the box at the
16 bottom left labeled "30."

17 A. I see it.

18 Q. What's your understanding of what this box
19 represents?

20 A. According to the reference, it's a central
21 patient data processing system.

22 Q. And the central patient data processing
23 system -- excuse me -- receives de-identified healthcare
24 information, or patient data, from the healthcare
25 entities (20); is that correct?

1 A. That's the way it's depicted in Figure 1.

2 Q. And those healthcare entities are the entities
3 that create the encrypted IDs, correct?

4 A. They have an encryption system, so they can do
5 the de-identified data, yes.

6 Q. Is part of the de-identified data that's
7 released by the healthcare entities to the central
8 system (30), does that include the encrypted IDs?

9 A. Looks like it does. I mean, again, it
10 wouldn't make sense to not have encrypted IDs if you're
11 going to want to retrieve that data. I mean, I guess
12 you could implement it without them, but I would expect
13 encrypted IDs to be there.

14 Q. All right. You've cited in your declaration a
15 number of times Exhibit 2006, which is the text of the
16 HIPAA Privacy Rule, correct?

17 A. It's cited in my dec, yes.

18 Q. So I'd like to pull that up. We looked at
19 that earlier.

20 Do you have that available?

21 And let's turn to -- on page 2 of
22 Exhibit 2006, there's subsection (c), "Implementation
23 Specifications: Re-identification."

24 A. You said Section 2?

25 Q. I'm sorry, page 2 -- on page 2,

1 subsection (c), about a third of the way down the page.

2 A. Got it.

3 Q. Okay. And this section provides that the
4 "covered entity may assign a code or other means of
5 record identification to allow information de-identified
6 under this section to be re-identified by the covered
7 entity," correct?

8 A. Yes.

9 Q. And then there's two provisions beneath that
10 that are requirements for this code or other means of
11 record identification that can be used for
12 re-identification, correct?

13 A. Yes.

14 Q. And the first one is the derivation
15 requirement.

16 Do you see that?

17 A. Yes.

18 Q. And the second one is the security
19 requirement.

20 Do you see that?

21 A. Yes.

22 Q. Would you agree that a system that allowed for
23 re-identification would need to abide by the provisions
24 in subsection (c) to comply with HIPAA?

25 A. Well, unless they had an agreement in place.

1 Q. In paragraph 23 of your declaration -- again,
2 your second declaration -- you noted that Landi
3 explicitly states that its design presents, quote, "no
4 HIPAA issues."

5 Do you see that?

6 A. Yes.

7 Q. And then the next sentence, you say, "A POSA
8 would have no reason to doubt Landi's statement in this
9 regard."

10 Correct?

11 A. Well, also, you left out that its goal is
12 HIPAA compliance, but, yes.

13 Q. Yeah. The full sentence, for the record,
14 states, "A POSA would have no reason to doubt Landi's
15 statement in this regard, particularly where Landi
16 describes a de-identified database."

17 Correct?

18 A. That's what it says.

19 Q. Would a POSA have reviewed the text of the
20 HIPAA Privacy Rule to verify whether Landi's assertions
21 about HIPAA compliance were accurate?

22 A. Probably.

23 Q. Would a POSA ordinarily take at face value a
24 patent's representations about HIPAA compliance?

25 A. Well, they would have knowledge of HIPAA

1 compliance. I wouldn't say take at face value. They'd
2 make an informed decision.

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

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

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

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

16 Q. All right. Well, let's -- I'd like to turn
17 back to 2006, then, Exhibit 2006, and look at the HIPAA
18 re-identification rule.

19 Under the derivation provision, this provides
20 that a code or other means of record identification
21 cannot be derived from or related to information about
22 the individual, correct?

23 A. That's what it says.

24 Q. And as we reviewed earlier, Landi's encrypted
25 ID is derived or relates to information about that

1 individual, correct?

2 MR. OLIVER: Object to foundation.

3 THE WITNESS: No, that's false. That's
4 factually false, and you know it. That's one particular
5 embodiment, as we discussed.

6 Stop.

7 BY MR. STEPHENS:

8 Q. Are there other embodiments that you're aware
9 of in Landi that do not use information derived or
10 related to an individual to create the encrypted ID?

11 A. It's certainly -- one skilled in the art would
12 certainly know that that's possible. I mean, you don't
13 have to derive it that way. In the public key example
14 that they gave, you could derive it that way, in which
15 case, you would need a business agreement.

16 Q. Let's take that example where the encrypted
17 ID -- in fact, I'll refer to Landi at, again, column 5,
18 line 7 through 19.

19 And at line 16 of this paragraph, it says,
20 "The patient identifying information, which is encrypted
21 to generate the encrypted ID, may include one or more
22 items of patient identifying information, including, but
23 not limited to, patient name, Social Security number,
24 and/or address."

25 Do you see that?

1 A. Yes. We've already discussed that.

2 That's true for that particular embodiment,
3 and so if you chose to do that, in order to maintain
4 HIPAA compliance, strictly speaking, you would need some
5 sort of associate agreement.

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

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

14 MR. STEPHENS: All right. We've been going
15 for about an hour again. I don't believe I have much
16 longer, but if we could take 15 minutes, I'll gather my
17 notes, and we can come back for -- to wrap up, if that's
18 okay.

19 THE WITNESS: Yeah, that's fine. Do you want
20 to try -- do you want more time, do it at 1:00, or --

21 MR. STEPHENS: Would you like a lunch break,
22 or we could come back at 1:00?

23 THE WITNESS: No, no, no. I don't need a
24 lunch break. I'm just trying to give you enough time to
25 do what you need to do.

1 MR. STEPHENS: No, I appreciate that. I'll be
2 fine. Let's take 15 minutes. How about we come back at
3 12:50?

4 THE WITNESS: Okay. I'll be ready.

5 MR. STEPHENS: Okay. Thanks.

6 (Recess: 12:33 p.m. to 12:51 p.m.)

7 BY MR. STEPHENS:

8 Q. Dr. Clark, have you discussed the substance of
9 your testimony at any point today or during this
10 deposition with counsel?

11 A. Not with anybody.

12 Q. I'd like to turn to paragraph 25 of your
13 second declaration. And this paragraph begins with a
14 discussion of the combination of Dick, Landi, and
15 Murphy.

16 A. Yes.

17 Q. In paragraph 25, the fifth line down, you
18 mention that, "If the minimum number is not met
19 (e.g., 3), in the example, a message indicates that the
20 number of hits is, e.g., '<3.' Where the query was for
21 the number of patients having a specific diagnosis, the
22 message does not answer the query."

23 Is that what you stated?

24 A. That's what it says.

25 Q. What's the significance of this -- what you

1 characterized as a minimum number in Murphy?

2 A. It meets a claim limitation in one of your
3 defendant claims where there's a thresholding for a
4 number of records.

5 Q. So this minimum number is like a threshold is
6 your opinion?

7 A. Right. You don't return the records if the
8 number is less than the threshold.

9 Q. And what's the number that you're comparing
10 against the threshold?

11 A. The example in Murphy is 3.

12 Q. In the example, the threshold would be 3. But
13 what number is compared -- what's the -- what are you
14 comparing to that number?

15 A. The number of records.

16 Q. The number of records returned in response to
17 the query?

18 A. Yes.

19 Q. And, again, you stated that, when the minimum
20 number is not met, the message does not answer the
21 query; is that right?

22 A. The records are not returned, so it gives you
23 an error message instead, number less than 3 -- whatever
24 the threshold is.

25 Q. What happens if the number is -- the number of

1 records is greater than the threshold?

2 A. Then I would expect it to return the number or
3 the -- and/or the records, depending upon the
4 implementation.

5 Q. So when the -- when the number of records
6 identified in response to the query is more than the
7 minimum number, then Murphy would either return the
8 number or the records themselves?

9 A. That would be my expectation. I mean, there
10 may be other disclosures. Yet, like all the other
11 references, I haven't memorized it.

12 Q. Now, would you agree, though, that when
13 that -- when the number is greater than the -- greater
14 than the threshold -- excuse me -- that the result
15 returned to the user in Murphy is obfuscated?

16 (Court reporter requested clarification.)

17 THE WITNESS: I don't know from memory. We
18 can go to the reference if you feel that's important.

19 The purpose of the reference is merely to show
20 that people knew about thresholding as a means to
21 prevent disclosure of sensitive information.

22 BY MR. STEPHENS:

23 Q. Yeah, let's turn to the reference. Do you
24 have a copy, or would you like me to put it in the chat?

25 A. Hold on. Let me see. I'm pretty sure I've

1 got it.

2 Q. Exhibit 1009.

3 A. Got it.

4 Q. And I'll refer to page 553 in Murphy.

5 A. Okay. I'm there.

6 Q. Okay. At the bottom of the right-hand column,
7 under the section titled "Methods," the third to last
8 line in that column, there's a sentence that begins, (as
9 read) "The method works by having the server not pass
10 true numbers of the patients to the query tool but
11 rather numbers that would be (if the same query were
12 returned [sic] repeatedly) distributed around the true
13 number of patients."

14 Correct?

15 A. That's what it says. It says at the start of
16 that paragraph, "In an abstract sense, the key to the
17 data obfuscation" --

18 So, I mean, I'm not sure what you're driving
19 at, but I think we probably need the whole context.

20 Q. And in the context of that paragraph, would
21 you agree, though, that the number of patients that's
22 returned to the user in response to a query is not the
23 true number of patients that were identified?

24 A. That's what that paragraph says, yeah.

25 Q. And Murphy refers to that as obfuscation,

1 correct?

2 A. That's what it says.

3 Q. So the users returned an obfuscated result
4 even when the number of results identified is greater
5 than the minimum number, correct?

6 A. In that particular case, yes. Doesn't have to
7 be that way. I mean, the disclosure doesn't require
8 that.

9 Q. And at page 555, in the right-hand column, at
10 the last sentence of the paragraph that begins with
11 "although," it states, (as read) "Therefore, we modify
12 our range algorithm to have a wider obfuscation at
13 values close to 0 and indicate the greater range by
14 returning '<3' when the obfuscated number is less than
15 3."

16 Correct?

17 A. That's what it says.

18 Q. So when the obfuscated number is less than the
19 threshold, it returns an indication that the value is
20 less than the threshold, correct?

21 A. Well, I mean, that's a possibility. That's
22 one of the disclosures that the reference gives.

23 Generally speaking, it's talking about the use
24 of thresholding.

25 Q. This is the disclosure that was cited in your

1 first declaration, correct?

2 A. Murphy has been the reference used to
3 demonstrate that thresholding was known to one of skill
4 in the art at that time.

5 Q. So what I'm driving at is that Murphy is
6 saying here that the result returned to the user is
7 obfuscated both when the result is less than the
8 threshold and greater than the threshold; is that
9 correct?

10 A. That's one possibility that you -- I mean,
11 it's talking about generally, as I said, thresholding,
12 and so one possibility is to never return an exact
13 number.

14 Q. There's an obfuscated result regardless of
15 whether it's above or below the threshold, correct?

16 A. That's one possibility.

17 Q. But the obfuscation range may be greater when
18 the result is less than the threshold, correct?

19 A. I'm not sure that's true. I mean, that's an
20 example that's possible. I mean, they are talking
21 generally about the threat to returning small numbers of
22 records.

23 MR. STEPHENS: All right. I have no further
24 questions.

25 MR. OLIVER: I have a couple of just very

1 brief questions.

2 EXAMINATION BY MR. OLIVER:

3 Q. Dr. Clark, in a public/private key system,
4 does the public key -- or is the public key used to
5 encrypt information?

6 A. It can be. In RSA, an example, that is one
7 possibility.

8 Q. And the private key is the means for
9 decrypting the information, correct?

10 A. Yes. The access to the private key is
11 required to decrypt information in a public key system.

12 Q. And that private key can be used to decrypt
13 any information encrypted by a public key, correct?

14 A. Generally speaking, for RSA, that's true.

15 MR. STEPHENS: Counsel, I'd remind, on
16 redirect, this should be nonleading questions.

17 BY MR. OLIVER:

18 Q. Does the private key depend in any way on the
19 specific information -- let me rephrase that.

20 Do the public and private keys -- or are they
21 created prior to the encryption and decryption being
22 performed?

23 A. Generally speaking, yes, but it's not a
24 requirement.

25 MR. OLIVER: I have no further questions.

1 MR. STEPHENS: Nothing further.

2 COURT REPORTER: Counsel, may I get transcript
3 requests on the record, please?

4 Mr. Stephens, I do have your request.

5 MR. STEPHENS: Okay. Thank you.

6 MR. OLIVER: I don't need a copy. One will be
7 filed in the record, so I don't need a rough or final,
8 for that matter.

9 MR. STEPHENS: Would you mind reminding me
10 what our order was?

11 COURT REPORTER: May we go off the record?

12 MR. STEPHENS: Off the record, please.

13 (Whereupon the proceedings concluded at
14 1:05 p.m.)

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: JANUARY 16, 2025
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 January 16, 2025; 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

STATE OF CALIFORNIA)
) ss.
)

**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, prior to being examined, the witness named in the foregoing deposition was by me duly sworn to testify to the truth, the whole truth, and nothing but the truth;

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;

That the dismantling, unsealing, or unbinding of the original transcript will render the reporter's certification null and void.

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

In witness whereof, I have hereunto subscribed my
name.

Dated: January 20, 2025.

Zamarra T. Houston

TAMARA L. HOUSTON
CSR 7244, RPR, CCRR 140

THE SULLIVAN GROUP OF COURT REPORTERS

	10:17	12:13 19:6 24:5 66:15, 22 69:17	47 37:25 39:23 40:2
(	10:05 6:1	2007 10:16	
(20) 65:25	11:11 40:14	2007/0294111 13:6	5
(30) 66:8	11:30 40:8	2024 8:11	5 31:15 34:5 63:10 70:17
(b)(2)(i) 19:13	11:34 40:14	2024-00226 7:11	553 75:4
(c) 66:22 67:1,24 69:10	12 40:16 53:7 56:3	2025 6:1	555 76:9
(e) 24:6	12:33 72:6	23 58:5,9 63:2 68:1	56 64:11
(e)(2) 24:16	12:50 72:3	25 72:12,17	
	12:51 72:6		6
-	15 40:6 52:5 64:19 71:16	3	6 64:10
--o0o-- 6:2,9	72:2	3 11:8,10 24:7 64:18 72:19,20 73:11,12,23 76:14,15	641 7:11 26:21
	16 6:1 70:19	30 20:25 29:16 65:12,16	
0	17 58:7	304 32:1,6 34:10,16	7
	18 64:19	308 32:6	7 31:15 63:10 70:18
0 76:13	19 61:24 63:10 70:18	312 32:5	7244 6:4
	1:00 71:20,22	38 11:20 13:3 34:3	
1	1:05 79:14	39 11:24 12:20 13:2,9 16:20 17:1,3,9 19:2,20 20:1,5,10 50:22 51:9,12	A
1 64:20 65:11,14 66:1			a.m. 6:1 40:14
1003 49:4,11,17	2 38:21,22,23 66:21,24, 25	4 63:16	abide 67:23
1005 10:16	20 63:2	40 11:20 17:1 20:25	ability 25:24 29:14 37:22
1006 12:2,12,13	2001 10:16	41 31:20	absolute 30:12
1008 63:8	2003 12:10		Absolutely 48:1
1009 10:16 75:2	2006		abstract 75:16
1014 10:17			accept 7:22 30:16
1015 7:14			access 18:6,19,25 19:1,2 24:15 27:14 28:25 37:2 44:9 45:13 46:5 47:1 52:17
1016 12:14			
1024			

Index: (20)-access

THE SULLIVAN GROUP OF COURT REPORTERS

54:7,9 55:11 56:18 78:10	agree 15:9 16:12 27:7 55:15 67:22 74:12 75:21	arguments 30:13	26:7
accessed 64:22	agreement 28:13 41:14,20 42:12, 18 43:3,9,13,16,19,24 44:6,16,22 45:15,17 46:2,6,10,21 47:13 52:13 53:3,9,15,23 54:3,12,15,16,21,23 55:16,21,24 56:15,24, 25 57:13 58:1 67:25 70:15 71:5,7,12	art 16:21 17:12,20 25:22 70:11 77:4	authorized 22:15 64:22
accessible 53:17		aspect 58:20	avoid 52:22,25 53:20 56:1
accessing 18:20		asserted 52:21 58:25	aware 7:24 9:5 15:3 43:18 70:8
accurate 68:21		assertion 55:5,14	B
accusing 30:20	agreements 43:25 44:3 47:4,23 52:7 53:20 55:3,12,13,25 56:4 57:7 58:18 60:17 61:2 69:13	assertions 68:20	BAA 41:19,20,23 52:22
achieve 61:4 62:16		assess 23:2 47:13	back 16:20 39:23 40:7 52:5 69:17 71:17,22 72:2
acknowledges 62:4	alg- 34:1	assessment 23:7 44:11	back-end 48:12 50:24
acronym 53:4	algorithm 33:14,23 34:1 76:12	assign 67:4	bad 52:16 53:13
activate 38:14	alleged 26:20	assigned 34:8,17,21	based 14:18 19:24 20:18 25:8 32:1 51:1
actor 52:16 53:13	allowed 10:5 22:14 26:2 27:5 67:22 69:13	assigns 35:5	basically 36:9
actors 54:18	alternative 30:25	associate 40:20,22,25 41:12,14, 20 42:1,5,11,13,17 43:3,13,16,19 44:3,6, 14,16,22 45:7,11,17 46:1,5,9,21 47:1,13,23 52:7,13 53:3,8,15,23 54:3,14,15,22 55:16,20 56:4,15,25 57:13,22 58:1 60:17 61:1 69:13 71:5,7,12	begins 72:13 75:8 76:10
actual 8:25	analysis 17:11		behalf 6:17,23
ad 51:14 57:16	and/or 70:24 74:3		beneath 67:9
address 20:11 52:19 70:24	answers 30:1,20	associates 41:7 58:19 59:12,25 60:3	benefits 62:4
administering 54:18	appearance 6:22	assume 14:16 18:5	biography 69:8
administers 56:10	approaches 27:19,22,24 30:15	attacker 23:18	bit 40:4,5
administrative 34:9	architect 15:13	attain 35:13 61:18	bottom 63:15 65:12,16 75:6
administrators 36:7	architected 17:23 46:15 53:12	author 69:3	boundaries 39:2
advantages 15:2	architecture 47:19	authorization	box 65:11,15,18
aggregator 48:7,17,20 49:2 50:3,9, 21,24 51:6,9,20,23 52:12,16,17 54:20,23 55:21 56:10	arguing 20:6		boxes 39:11,13,21

Index: accessed-boxes

THE SULLIVAN GROUP OF COURT REPORTERS

break 40:4 71:21,24 broad 31:5 broader 21:21 broadly 17:16 business 40:20,22,24,25 41:7,12, 14,20 42:1,5,11,13,17 43:3,13,16,19 44:3,5, 14,16,21,25 45:6,10,17, 22 46:1,5,9,21 47:1,13, 23 52:6,13 53:3,8,15, 20,23 54:3,14,15,22 55:12,16,20 56:4,15,17, 25 57:13 58:1,19 59:12, 25 60:2,17 61:1 70:15 71:7 businesses 44:1	centralized 11:12 48:10 certifications 61:21 Certified 6:4 cetera 58:18 characteristics 34:7 characterization 60:4 characterized 73:1 chat 10:1 12:5,16 19:5 49:6, 16,21 74:24 check 27:25 69:3,9 cherry-picking 60:12 choice 15:24 choose 14:19,23 15:7,15,21 16:5,17 chose 71:3 cite 11:20 17:1,2 cited 26:16 66:14,17 76:25 city 20:11 21:20 claim 64:18,20 73:2 claims 26:21 73:3 clarification 11:1 74:16 clarify 18:14 clarity 49:18	Clark 6:5,11 7:2 10:11 11:5 40:6 49:17 72:8 78:3 classified 13:16 classify 24:20 clean 10:11,19 clear 17:7 30:2 44:2 59:7,13 60:21 clinically 11:13 close 76:13 Closed 9:22 code 20:12 67:4,10 69:20 codes 21:19 34:8 collaboration 9:1 column 34:5 63:10,16 64:10,19 70:17 75:6,8 76:9 combination 47:25 50:1,6,19 51:3, 16,23 52:8,13 53:7 54:16 72:14 combination's 50:8 combine 36:21 communication 9:20 compared 73:13 comparing 73:9,14 completely 7:6 compliance 14:6 15:4 27:22,23	46:16 58:11,14,15,20, 21 59:2,8,18,21 60:1,7, 8,14,22 61:2,5,8 62:10, 13,17,23 68:12,21,24 69:1,6 71:4 compliant 29:2,4 31:1 61:14,17,19 62:14,20 71:12 comply 15:7,10,13 16:13,15 27:24 42:1 55:3 56:20 60:24 67:24 69:10 complying 45:25 component 54:10 components 39:7,14,21 comprising 64:21 concept 40:20 42:10 concerned 15:5 16:9 50:8 62:9 concluded 79:13 concrete 47:16 confidence 33:8 confused 28:12 consideration 61:9 considered 22:7 consistent 17:9 contained 64:1 contemplates 14:16 62:5,22 contended 26:19 47:23 context
C			
calculated 34:20 California 6:4 call 9:9 36:9 called 6:6 49:19 54:6 calls 36:4 care 31:25 case 23:25 36:7 42:25 49:14 53:19 54:25 57:25 70:15 76:6 cases 6:15 44:15 CBA 52:19,25 53:2 central 39:10 46:7 51:23 65:20, 22 66:7			

Index: break-context

THE SULLIVAN GROUP OF COURT REPORTERS

75:19,20	8:5	4,11,14,23,24 58:2	declarations
contract	countermeasures	61:15 64:23 65:21,22,	8:6 48:24
41:6	28:2	24 66:5,6,11 75:17	decode
contracting	county	database	32:6,11,18,21,24
43:25 55:15	20:12	18:20,22 27:18 28:3	decrypt
contrary	couple	29:17 46:16 53:16	33:16 34:2 35:9 64:23
62:20	9:13 63:1 77:25	68:16	78:11,12
control	court	databases	decrypting
28:25	6:3 11:1 74:16 79:2,11	11:11	78:9
conversely	covered	dataflow	decryption
42:17	24:13 25:23 26:9 36:3,	50:19 51:5,8	64:21 78:21
cool	10 41:6,13,23 42:12,18	Datavant	defendant
60:20	43:1 52:2 53:4 55:1,17,	6:24	73:3
copies	22 56:5,11,13 61:10	dates	defined
10:11,19	65:8 67:4,6	11:15	40:25
copy	create	de-identification	definition
74:24 79:6	13:15,21 21:23 29:14	13:25 14:15 15:10,13	13:16
correct	33:11,19,22,25 63:21	17:10,21 19:8,25 25:15	definitions
7:21 9:21 11:21 13:22	66:3 70:10	57:6 62:5,24	30:12
15:11 16:14 20:14,19,	created	de-identified	degree
20 21:3 22:19 24:12,18	27:11 31:25 63:14	13:15,17,22 16:22,23	25:21
26:17,21 27:8 28:6,9,16	78:21	18:25 20:17 21:12,24	demonstrate
29:23 31:4,9 32:14,21	creates	24:25 25:6,10,18,21	77:3
33:8,11,19,22,25 34:14,	63:19	42:19 43:1,4,8,11,12	depend
18,23 35:6 36:12,24	creation	46:8,9,16 48:19 50:2	14:21 22:24 44:13 45:5,
37:10,13 38:8,14 39:2,	21:16 27:8 28:4,14	51:17 54:2 56:14 57:11	9,12 46:4 53:10 57:21
5,10,25 40:20 41:1,10	crown	64:23 65:4,23 66:5,6	78:18
42:2,14,20,21,24 43:13	51:1	67:5 68:16	depending
45:19 47:25 48:5,8,11,	D	de-identify	19:3 26:8 32:22 45:20
16 51:18,24 52:8 55:1,		14:19 15:15 18:4 28:2	52:18 53:11 65:6 74:3
23 56:21,24 57:4,14,18	data	41:25 57:3	depends
58:2,3,22 59:18 63:14,	13:15,17,22 14:19	de-identifying	17:22 24:23 25:11,18
20 64:5,8,15,25 65:8,25	15:16 16:22,23 20:17	22:2	27:9 28:10 35:3 36:13
66:3,16 67:7,12 68:10,	21:2,5,8,9,11,16,24	dec	37:9 42:5,15,16,21
17 69:22 70:1 75:14	22:3,7,10,21,24 23:8,	9:3 66:17	43:17 44:8 46:14,25
76:1,5,16,20 77:1,9,15,	14,21 24:12,17,20,23,	December	47:7,10,18 54:18 65:9
18 78:9,13	24 25:5,9,14,17,24	8:11	depicted
correctly	26:6,10,17,20 27:3,8,	decision	66:1
11:18	12,16,18 28:4,14,23	69:2	deployed
correspond	29:15,22,23 30:4,5,6	declaration	39:15
19:19	38:24 39:4,10,16 41:8,	7:10,14,20,25 8:2,9,10,	deposition
counsel	25 42:9,22,24 43:2,11,	14,22 9:6,10,15 11:6	6:14 7:3 9:8,12,21 49:8,
6:21 8:20 9:9 72:10	12,15,20 44:7,12,17,21	26:24 31:15 40:17	12,16,19 72:10
78:15 79:2	45:18 46:2,7,19,20,22	47:22 49:3,9,10,17	derivation
Counselor	47:5 48:7,10,13,15,18	50:5,15,23 52:6,15,21	67:14 69:19 71:13
16:19 22:23 44:23 59:6	49:1,2 50:1,2,3,20 51:5,	53:8 55:5,7 57:18 58:6	
60:20 69:8	8,11,16,17,19,23,24	61:24 63:1 66:14 68:1,2	
count	52:1,4,12 53:6 54:6,20,	69:4 72:13 77:1	
	23 55:21 56:14,15 57:2,		

Index: contract-derivation

THE SULLIVAN GROUP OF COURT REPORTERS

derive 70:13,14	54:2	documents 9:25 10:1	13:13,23 17:4 19:1 20:6,20,21 32:19 33:9, 13,20 35:4,11 39:8,16, 20 63:16 64:16 65:1,6, 10 70:5 71:2
derived 64:7 69:21,25 70:9	disclosed 20:1 46:17 57:10	doubt 68:8,14 69:5,14	embodiments 17:3 30:25 36:14,20 38:9 40:1 70:8
describe 50:5,19 51:4 62:24	discloses 36:23	download 10:5 49:14	employ 54:6,13
describes 31:24 33:14 39:24 50:23 63:13,17 64:14, 16 68:16	disclosing 41:25 42:24 47:2 53:13 56:14 57:4	downloaded 13:7	employed 28:2 53:20
description 16:22 21:14	disclosure 22:18 26:6,16,19 27:3 32:2 36:15 43:12,15,20 44:17,21 45:18 46:2,21 47:5 57:13,21 58:1 74:21 76:7,25	downsides 53:22	employing 53:22
design 58:10,24 59:7 61:13 68:3	disclosures 74:10 76:22	draft 8:23	EMR 34:8,13,17,23 35:5 37:14,16,17 38:6,16,21 39:19,25 40:2
designed 55:19	discussed 48:25 51:14 57:16 58:4 62:16 65:2 70:5 71:1 72:8	drafting 8:23	EMRS 39:1,4,9
designer 15:19,24 16:9	discusses 11:12	driving 75:18 77:5	encoded 31:14,17
designers 15:1,7	discussing 35:17 57:19	drop 10:1,4 11:2 12:5	encrypt 27:13 33:15,19 34:2 63:25 78:5
designing 54:8	discussion 11:6 25:2 31:14 42:22 72:14	dropping 31:11	encrypted 51:14 63:3,14,20,22 64:3,7,23 65:3 66:3,8, 10,13 69:9,24 70:10,16, 20,21 71:8 78:13
determine 23:8,18	discussions 8:16	E	encryption 34:1 66:4 78:21
diagnosis 11:16 72:21	distinct 39:4,9	e.g. 58:19 72:19	end 11:14
dialogue 38:6	distinction 25:9	e.g. 72:20	engineering 27:19,21 30:15
Dick 61:25 62:3,5,9,22 72:14	distinguish 24:24	earlier 16:7 35:8,18 36:2 54:4 66:19 69:24	enter 38:13
Dick's 62:12,14,19,21	distributed 75:12	easier 10:10,22 12:18	entire 50:15
difference 21:10	docs 10:8	easy 55:9	entirety 26:25
difficulties 12:22	doctors 36:7	efforts 61:23	entities 24:14 29:7 35:2 36:10 41:7 48:4,15 50:2,20 51:5,18,22,24 52:1,2 54:15,25 56:5,7 65:25
digits 20:13	document 12:9 49:8,12,16	elect 17:20	
direct 28:5,15 29:19	documentation 11:16	Electronic 38:19	
disclose 22:15 23:10 25:24 26:10 27:5 36:17 42:4, 12,19 43:4 44:6 46:10		eligible 54:21	
		emails 9:22	
		embodiment	

Index: derive-entities

THE SULLIVAN GROUP OF COURT REPORTERS

66:2,7	exhibits 10:16,17	field 31:6	functionality 50:6
entitled 17:24	expect 10:23 35:24 52:3 53:10 66:12 74:2	fields 25:15 27:13	functions 41:7 47:19 57:22
entity 26:10 33:10 36:3 40:23 41:6,14,24 42:12,18 43:1 55:1,17,23 56:5,13 63:25 64:3,22 65:5,7,8 67:4,7	expectation 74:9	figure 38:21,22,23 39:3 65:11, 14 66:1	
entity's 25:24	experience 16:3 29:16,20	file 10:7,13 49:19	G
EPID 31:16,24 32:6,21 33:3, 11,19,22,25 35:9,14 36:12 37:23 38:12,13 39:25	expert 69:4	filed 79:7	gather 71:16
EPIDS 36:24	explain 18:9 45:8	files 9:16 10:15	gathering 47:11
error 73:23	explains 32:4 38:4 63:24	final 79:7	gave 16:8 31:2 70:14
errors 9:5	explicitly 50:12 58:9 68:3	find 35:23 38:6 63:7	general 36:5 46:13,15 58:17 61:12
established 8:17	extent 52:25 53:11 56:18 60:16,25	fine 8:13 10:21 71:19 72:2	generally 42:8 51:13 53:17 54:11 62:5,22 76:23 77:11,21 78:14,23
evaluations 23:12	F	fixed 9:7	generate 64:3 70:21
Evenhaim 11:12 48:23 51:2,4,14	face 68:23 69:1	folder 10:11,14 12:3,9	generated 57:23 71:7
Evenhaim/settimi 47:24 49:25 52:8	fact 52:16 70:17	form 23:23 26:22 33:12 43:6 59:4	geographic 20:10,18 21:21
exact 77:12	factually 70:4	found 49:22	give 27:2 30:1,3 47:15 71:24
examination 6:10 11:15 78:2	fall 18:2,7	foundation 33:12 59:4 70:2	giving 30:20
examples 23:5 41:2 47:16 57:8	false 70:3,4	fourth 46:24	goal 53:11,14 54:4 58:11 59:2,8,17,20 60:5,7,14, 21 61:3 62:21 68:11
excuse 60:6 65:23 74:14	familiar 13:24 14:11 17:12,14 21:5	free 10:2,12	goals 62:12
exemplary 13:13 17:3 30:25 63:16	fashion 29:2,19	front-ending 38:24	good 6:11 59:11 60:18
exhaustive 41:3	faster 12:24	full 68:13	grab 11:3
exhibit 7:13,14 12:1,2 19:6 24:5 49:4,11,17 63:8 66:15,22 69:17 75:2	features 62:14,20	fully 13:16,21 16:22 18:24 43:8,11,12,23 46:8 56:14	granular 20:22
	feeding 39:16	function 38:7	greater 74:1,13 76:4,13 77:8,17
	feel 10:2,12 74:18		guess 16:20 18:13 28:12,22

Index: entitled-guess

THE SULLIVAN GROUP OF COURT REPORTERS

58:8 66:11	21,22,25 61:2,4,8,11, 13,17,21 62:4,9,12,14, 17,20,23 65:8 66:16 67:24 68:4,12,20,21,24, 25 69:4,6,11,17 71:4,10	identity 35:14	36:2 37:8 64:8 69:22 70:1,10
guideline 30:14		IDS 63:3,14 66:3,8,10,13 69:10	individuals 17:24 20:17 22:15 24:14 29:6 36:5
		imagine 44:18	induction 61:18
H	HIPAA's 13:24 27:16	implement 17:18,25 24:1 27:11 28:18 29:2,18 30:15,23 62:13 66:12	industry 61:18
halfway 13:11 34:6	HIPAA-COMPLIANT 29:19 30:15 69:15	implementation 16:10 25:19 39:22 51:21 52:19 63:17 66:22 74:4	information 11:14 18:6 21:17,24 22:2,3,5,8,13,14,18,22 23:3,9,14,20,22 24:17, 21,25 25:6,10,18 27:6, 7,12,20 28:9 29:6,9,21 30:5,10 31:3,6,7,11 35:16,19,23,24 37:5,7 41:13 42:13,19 43:5 46:8,9,10 48:14,15,19 50:2,10 51:17 54:2,10 56:18 57:10 64:1,8 65:4,24 67:5 69:21,25 70:9,20,22 74:21 78:5, 9,11,13,19
handle 41:8,12	hits 72:20	implemented 14:22 23:17 25:12,13, 14 27:10 32:22 35:15 36:13 37:9 69:14	informed 69:2
harbor 13:24 14:3,5,7,18,20,23 15:3,16,21 16:5,10,17, 24 17:9,13,20 18:3,8, 11,15,18 19:9,16 20:2 21:9,12,14,17,21,25 22:4 42:23,24 43:2,23 57:9,12	Hold 74:25	implementer 15:25	instance 17:1 43:4
hardware 39:22	hour 40:4 71:15	implementers 15:6	instances 23:13,19,21 45:16
health 22:8,12,18,22 23:2,9, 14,20,22 24:17,21 41:13 42:13	hours 9:11	implementing 61:10 62:19	intended 56:1
healthcare 41:8 63:24 64:3 65:5,7, 23,24 66:2,7	Houston 6:3	important 32:9,16 61:8 74:18	interconnected 51:10,25
heard 14:1	hypothetically 16:2	importing 51:17	interconnection 50:23
helpful 50:4,14 61:23		imposes 22:17 25:23 27:3	interrupt 12:8
higher 22:1	I	improperly 24:1	introductions 6:15
HIPAA 13:16 14:8,10,11,14 15:10,14 16:13,15 17:10 19:7 21:3,6 22:8, 13,17 23:11,15,22 24:12,20,24 25:7,10,23 26:10,15 27:3,23,24 28:4,15,17 30:13,18 36:3,4 40:20 41:1,9,13 42:1,11 43:14,16,18 44:1,4,7,12,20 45:19 46:1,17 47:6 52:2,20,23 53:1,18,20 55:3,11,12, 13,18,19 56:1,21,22,23, 25 57:15,24 58:10,11, 14,15,20,21,24,25 59:3, 7,8,17,21,25 60:7,8,14,	ID 63:20,22 64:4,7,23 65:3 69:25 70:10,17,21 71:8	individual 23:25 31:9 34:22 35:21	invention 13:13
	ideally 54:7		invoking 38:6
	identification 67:5,11 69:20		involved 8:21 18:1
	identified 57:17 74:6 75:23 76:4		
	identifier 31:18 32:1,14 34:9,16, 17 37:10		
	identifiers 13:14,21 19:14,19,20 20:8 21:22 28:5,8,15, 20,21 31:14		
	identifies 34:22 37:12		
	identify 16:4 37:22		
	identifying 34:7 37:5,7 64:1 70:20, 22		

Index: guideline-involved

THE SULLIVAN GROUP OF COURT REPORTERS

involving 7:11	13:6 65:12,16	lines 63:10	30:12 54:11 55:9 58:24 62:15 66:10 69:2
IPR 7:11,15,21,25 8:3,7	lack 33:24	lining 20:4	making 15:23
issue 59:8	lacked 33:10	list 13:20 19:14	managing 61:15
issues 59:8	Landi 58:9 59:1 60:5 61:4 63:6,11,19,24 64:18 65:7,11 68:2,15 69:3 70:9,17 72:14	listed 19:20 39:7	manner 69:15 71:8
issues,' 58:10	Landi's 58:24 59:17 60:5,7,21 63:2,13 64:7 68:8,14,20 69:5,9,24 71:8	location 20:22	marked 7:14
issues.' 68:4	laptop 9:16	logical 39:21	matched 19:23
items 64:1 70:22	leaked 33:1	long 34:4	materials 9:14
	leaving 8:23 21:22	longer 31:8 71:16	matter 45:25 47:3 79:8
J	left 34:4 65:12,16 68:11	looked 66:18	means 56:12 65:3,4 67:4,10 69:20 74:20 78:8
January 6:1	length 48:25	loss 22:2,3,5 27:7,12 28:9 30:10 31:6,7,11	meant 21:1
Justin 6:23 40:10 49:15	level 18:4 61:16	lot 27:21	mechanisms 26:9 59:24 62:25
	levels 57:6,8	lots 15:12 16:15 17:4 27:19 28:1 29:1,18 30:14,22, 24 62:16	medical 38:19 64:2
K	liability 15:5 16:9,14 43:22 57:20	low-resolution 11:11	meet 27:15
keeping 8:4	likewise 33:21	lower 29:22 30:4	meets 73:2
key 33:15 63:17,22,25 64:22 70:13 75:16 78:3, 4,8,10,11,12,13,18	limb 29:17	lunch 71:21,24	memorize 14:12
keys 78:20	limitation 73:2		memorized 14:17 21:7 26:14,25 74:11
kind 23:1 26:1 30:1 45:14 50:16	limited 21:2,5,11,16,20,24 22:7,21 23:8,14,21 24:12,17,20,24 25:5,9, 17,24 26:6,10,16,20 27:3,8,12,16 28:4,14 29:15,22 30:3,6 42:22 43:15,20 44:6,12,17,21 45:18 46:2,19,20,22 47:5 57:24 58:2 70:23	M	memorizing 17:14
kinds 24:1		made 69:12	memory 14:2 18:18 25:1 74:17
knew 21:1 74:20		maintain 61:2 71:3	mention 72:18
knowledge 68:25		maintained 34:14	mentioned 19:5 35:8 36:1 49:25
		maintaining 64:21	message 72:19,22 73:20,23
L		make 6:22 12:17 18:3 23:7	
lab 11:16			
labeled			

Index: involving-message

THE SULLIVAN GROUP OF COURT REPORTERS

messages 9:22 met 72:18 73:20 method 13:25 14:4,7,19,20,24 15:3,16,21 16:5,17,24 17:8,9,13,20,21 19:9, 16,25 20:2,9 21:12,17, 25 22:4 43:2 57:9,12 64:20 75:9 methods 14:15,24 15:17,22 16:6, 12,18 62:6,23,24 63:23 75:7 mind 8:6 13:3 26:12 29:13 44:5 47:12 79:9 minimize 42:8 54:7,9 minimum 14:6 15:4 72:18 73:1,5, 19 74:7 76:5 minutes 40:6 71:16 72:2 mixing 36:14 Mm-hmm 63:5 modify 76:11 moment 64:12 month 8:11 morning 6:11,13 motivated 62:13 multiple 14:9 39:16 Murphy 72:15 73:1,11 74:7,15 75:4,25 77:2,5	N Names 23:6 nauseam 51:14 57:16 necessarily 18:21,25 23:16 27:25 28:3,10 29:24 33:5 39:6 42:3,21,25 52:24 53:18 57:5 58:3,23 59:22 needed 42:18 54:13,24 Nick 6:16 10:10 nonleading 78:16 noted 68:2 notes 9:18 34:3 71:17 number 6:4 9:25 12:1 38:13 47:9 48:4 54:17 66:15 70:23 72:18,20,21 73:1, 4,5,8,9,13,14,15,16,20, 23,25 74:2,5,7,8,13 75:13,21,23 76:4,5,14, 18 77:13 numbers 23:6 34:7 75:10,11 77:21	52:15 59:4 objective 37:3 60:10 obtain 56:18 obviate 54:12 obviousness 26:21 51:1 occur 52:23,24 offered 25:5,7 61:22 Oliver 6:23 10:10 12:8,11,15 23:23 26:22 33:12 36:25 40:11 41:17 43:6 46:11 49:18 59:4 70:2 77:25 78:2,17,25 79:6 one-size-fits-all 47:20 open 9:17 10:7 opened 10:15 opinion 55:10 73:6 opinions 8:17 9:3 25:5,7 55:8 opposed 8:23 14:24 15:16,21 16:5,17 21:24 options 36:19 58:23 order 13:15 30:12 32:6 33:15, 18 71:3 79:10 ordinarily 68:23 original 29:23 30:5 origination 51:19 overload 53:5	owned/managed 64:2 owner 6:17 owns 56:10 P p.m. 72:6 79:14 paragraph 11:8,10,24 12:20 13:2, 9,12 16:20 17:9 19:2,20 20:1,5,10,18,24,25 21:2 31:20,24 34:3,4,6 37:1, 19,25 38:10,17 39:23 40:2,16,19 41:4 50:22, 25 51:9,12 52:5 53:7 56:3 58:5,9 59:7,13 60:12,13 61:24,25 64:11,14 68:1 70:19 72:12,13,17 75:16,20, 24 76:10 paragraphs 11:20 31:15 63:2 parse 60:19 part 66:6 particulars 47:2,8,10,15,18 parties 46:22 55:16,17,22 61:22 partition 27:18 party 33:2,3 42:19 43:5 44:7 45:6,10 46:10 pass 75:9 password 32:1,4,9,17,25 33:1,4,7, 10,15,18,24 35:8 36:11 patent 6:17 7:11 13:1,4 26:21
---	--	--	---

Index: messages-patent

THE SULLIVAN GROUP OF COURT REPORTERS

patent's 68:24 patents 24:3 path 51:19 patient 26:5,7 31:4,14,17,25 32:1,13 33:4 34:9,16 35:5,14 36:12 37:10,13, 23 38:5 39:24 41:25 43:2 57:3 64:1,2,4,24 65:21,22,24 70:20,22, 23 patient,' 11:14 patients 27:6 36:24 72:21 75:10, 13,21,23 PAUL 6:5 PCP 31:25 32:5,10,17 33:7 34:8,14,17 35:2,5,13,22 36:11 37:13,17 38:18 39:2,19 PCPS 36:23 39:2,16 48:15,19 pdf 24:7 people 18:1,6,7,14,19 24:15 36:6 74:20 performed 78:22 permission 26:3 person 16:21 17:12,19 25:22 36:20 56:10 perspective 42:7 44:25 45:22 pertaining 44:3 61:25 pertains 50:25 60:4	Petitioner 6:21 phrased 28:7 phrases 60:12 PID 32:6,12,13,18 33:16,19, 21,24 34:10,16,22 35:1, 5,9,23 37:2,5,7,10 PII 17:25 18:19 19:1 22:10 23:4,5,11,18 24:15 52:17 53:13 55:11 56:19 place 26:24 28:25 41:19,23 43:9 44:16 45:15 46:2 55:13,21 56:4,19 57:1,7 67:25 71:7 places 14:9 63:1 plain 28:24,25 plan 40:7 point 26:23 48:22 50:4 72:9 pointer 28:24 29:1 populate 50:10 POSA 68:7,14,19,23 69:5 POSITA 14:19,23 15:15,21,23 16:17 19:25 39:12,18 61:9 62:13 possession 33:3 possibilities 45:24 possibility 76:21 77:10,12,16 78:7 potentially 29:24,25 33:5,6	precinct 20:12 preferred 54:1 prepare 8:14 9:8 preparing 9:11 prescription 11:16 present 13:13 presents 58:10 59:7 68:3 pressed 10:24 presumption 18:5 pretty 16:25 22:23 24:1 59:13, 15 74:25 prevent 53:13 74:21 previously 65:2 prior 78:21 privacy 14:8,11,14 19:7 25:7 28:15,17 58:15,21 59:3, 10,21 60:1,9,15,23,25 62:17 66:16 68:20 69:11 71:10 private 78:8,10,12,18,20 privilege 54:6 proceeding 8:15 49:10 proceedings 79:13 processes 62:6,23 processing 65:21,22	properly 23:17 protected 22:7,12,18,22 23:2,9, 14,20,22 24:17,21 29:5 35:16,19 41:8,13 42:13 61:15 provide 14:14 provider 31:25 40:24 54:19 55:25 56:6,13 57:2,3,11 providing 36:19 provision 69:19 71:9 provisions 43:18 44:12 67:9,23 69:10 public 27:14 63:17,22 70:13 78:4,11,13,20 public/private 78:3 publicly 53:17 pull 18:10 48:14 66:18 69:7 purpose 46:15 55:4 61:6 74:19 purposes 34:9 pursue 17:20 put 19:5 28:23,24 49:6,13 55:8 56:19 74:24 Q qualified 23:2,8 qualifies 22:22 queries 49:2 50:9 51:13,15
--	---	---	---

Index: patent's-queries

THE SULLIVAN GROUP OF COURT REPORTERS

query 72:20,22 73:17,21 74:6 75:10,11,22 question 16:7 17:5 25:20 45:23 49:24 51:3 53:25 59:16 60:4,6 questions 6:17 7:7 10:3 44:2 63:3 77:24 78:1,16,25 quote 11:13,14,15 32:4 38:5 58:10 63:25 68:3	8:8 12:21 receive 42:9 48:14,18 49:1 50:1 receives 65:23 recess 40:14 72:6 record 32:13 35:6 40:13 64:24 67:5,11 68:13 69:20 79:3,7,11,12 records 38:6,19 39:24 41:25 42:1 64:2 73:4,7,15,16, 22 74:1,3,5,8 77:22 recover 35:9 redirect 78:16 reduce 28:3 reduces 22:3 refer 8:9 9:25 10:2 11:5 20:1 24:5,14 31:15 40:16,19 70:17 75:4 reference 10:22 11:6 13:5 19:4 30:23 48:24 56:12 61:6, 25 63:6 65:20 74:18,19, 23 76:22 77:2 referenced 14:10 references 24:3 29:13 74:11 Referencing 65:1 referred 18:14 31:3 58:14 59:17 63:2 referring 8:10 13:4 18:7,23 19:15 26:4 31:17 52:5 53:2 58:15 59:2 60:2 refers	21:2 24:11 38:16 75:25 regard 68:9,15 regulatory 27:22 related 6:15 40:24 69:21 70:10 relates 69:25 relating 9:15 relationship 45:6,10,21 47:19 released 66:7 relevant 26:20 remind 78:15 reminding 79:9 removal 20:22 21:17 28:5,14 remove 28:21 30:9 removed 13:14,21 19:14 20:9 28:11,24 29:10 removing 28:8 31:3,6 render 29:5 repeatedly 75:12 rephrase 53:25 78:19 replied 59:22 reply 7:10,14 8:10 55:5,7 reporter 6:3,4 11:1 74:16 79:2, 11 representation	7:23 representations 68:24 represented 7:17 represents 65:19 request 79:4 requested 11:1 74:16 requests 79:3 require 26:7 33:15 43:12,16,19 45:14 76:7 required 32:5 33:21 78:11 requirement 14:25 15:19 45:1,3,21 61:21 67:15,19 71:13 78:24 requirements 14:21 17:15 18:11 19:3, 8 24:11 27:16 30:17 67:10 requires 20:22 21:16 28:5,14 29:8 resolution 22:1 28:3 29:22 30:4 respect 46:19 respective 39:19 64:2 responding 7:6 52:21 55:4 response 18:14 28:13,20 44:23 73:16 74:6 75:22 responsible 9:3 responsive 52:15 restriction
R			
raised 52:15 range 76:12,13 77:17 re-identification 37:20 64:15,17 66:23 67:12,23 69:18 71:9 re-identified 65:5 67:6 re-identify 33:4 36:12,24 37:3,4 64:24 read 11:18 14:12 18:3 50:15 59:1 64:12 75:9 76:11 reading 36:19 reads 13:12 64:20 ready 72:4 realistic 52:18 reason 7:5 17:1 30:11 68:8,14 69:5,14 reasons 15:20 16:4,16 17:19 42:4 43:9,21 56:17 57:7,16,18,20 recall			

Index: query-restriction

THE SULLIVAN GROUP OF COURT REPORTERS

27:2	69:11,18 71:10	send 10:12	shown 38:21,22,23,24 39:1,9
restrictions 22:17 25:23 26:1 62:4	ruled 56:11	sending 42:6	shows 39:20
result 74:14 76:3 77:6,7,14,18	rules 25:7 41:1	sense 62:15 66:10 75:16	sic 75:12
results 76:4	S	sensitive 54:9 74:21	significance 72:25
results.' 11:17	safe 13:24 14:3,5,7,18,20,23 15:2,16,21 16:5,10,17, 24 17:9,13,20 18:2,8, 11,15,17 19:8,15 20:2 21:8,12,14,17,21,25 22:4 42:23,24 43:2,23 57:9,12	sentence 11:10 13:12 58:7 68:7, 13 75:8 76:10	simply 49:24
retain 28:22	sales 61:23	separate 25:2 39:7,11,13,14	single 30:8
retain[s 11:13	save 10:23	separately 35:17,20	sir 19:4 41:16
retained 28:11,20 35:25	scenario 56:2 71:6	server 75:9	site 51:19
retrieve 66:11	scroll 49:20	set 13:20 21:8,9,11,16,24 22:7,10,21,25 23:8,14 24:12,17,23 25:18 26:6, 10 27:8,12 28:4,14,23 29:15,22 30:4,5,6 43:15 44:7,21 47:6 57:24	sitting 8:8 26:12,14
return 73:7 74:2,7 77:12	search 20:16 38:5,7,12,14 40:2	sets 21:2,5 23:21 24:20,24 25:6,9,14,24 26:17,20 27:4,16,18 42:22 43:2, 20 44:12,17 45:19 46:3, 19,20,22 56:14 58:2	situation 42:16 44:14 45:5,9 47:2,8,11
returned 73:16,22 74:15 75:12, 22 76:3 77:6	searched 39:24	Settimi 11:6,20,24 12:1,20 13:5,20 16:21 19:20 20:1,10 30:23 31:18,21 32:4 34:3,5 36:17,22,23 37:21 38:1,4,16,21 39:23 48:11,23 49:1 51:4 52:7	sixth 41:5
returning 76:14 77:21	searcher 20:16	Settimi's 11:12 16:22 26:16 31:13	skill 16:21 17:12,19 25:22 36:21 77:3
returns 76:19	searching 12:7	short 31:25 41:20 46:13	skilled 70:11
reviewed 68:19 69:24 71:9	section 24:11 63:13 66:24 67:3, 6 75:7	Shorthand 6:4	small 77:21
right-hand 75:6 76:9	secure 29:17 54:5,6	show 74:19	smaller 20:11,18
risk 45:14 52:18,25 53:17	securely 27:20 37:5 64:21		Social 23:6 70:23
role 42:6	security 23:6 36:6 42:7,10 45:13 67:18 70:23		solution 29:3
rough 79:7	seek 21:23 61:13		sort 14:5 24:2 42:9 61:6 71:5
routinely 43:25	select 38:13		source 48:15 50:2,20 51:5,17, 24 52:1
RSA 63:17 78:6,14			speak 18:11
rule 14:8,11,14 19:7 28:15, 17 29:8 58:16,21 59:3, 10,21 60:9,16,23,25 62:18 66:16 68:20			

Index: restrictions-speak

THE SULLIVAN GROUP OF COURT REPORTERS

speaking 16:1 71:4,11 76:23 78:14,23	12 Stop 70:6	6:6 symmetric 32:24 33:14 63:22	test 11:16
specific 15:2,20 44:10,11 53:24 56:8 62:17,24 72:21 78:19	store 37:4	system 14:22,25 15:1,18,24 17:23 23:10,17 27:11 34:8,13,17,23,24 35:5 36:5 37:3,13,14,15,16, 17 38:18,19 39:5,10,19 42:5 46:15 47:20,24 48:5,12 50:24 53:12 54:5,8 57:22 61:10,13, 17,20 62:14,19 65:21, 23 66:4,8 67:22 69:14 78:3,11	testify 7:6
specifically 11:8 17:18 18:12 24:6 37:23 41:5,6 44:3 52:10 59:10	stored 46:8,20	systems 15:13 17:23 18:1 24:2 29:18 30:16,23 47:18 54:19	testimony 72:9
Specifications 66:23	storing 27:19		text 9:22 19:7 28:24,25 29:12 66:15 68:19
spend 9:11	straightforward 59:16		theory 55:2
stand 55:14	street 20:11		thing 50:8 59:11
standard 14:6 15:5 17:17 26:15 28:1 30:14 42:10 58:17	strictly 71:4,11		things 9:2 17:15 23:1 25:2
stands 60:13	strike 36:22 37:24 52:4		thought 59:15
start 38:10 75:15	string 32:5,9		threat 77:21
starting 58:8 64:11	study 30:8		threshold 73:5,8,10,12,24 74:1,14 76:19,20 77:8,15,18
state 11:11 20:11 21:20 30:9, 10 31:3,8,10,12 41:4,19 58:9 60:5 62:3	stuff 21:13 42:8		thresholding 73:3 74:20 76:24 77:3, 11
stated 59:22 72:23 73:19	subcontractors 36:8		Thursday 6:1
statement 55:4 68:8,15 69:5,12	subdivisions 20:10,19,22		time 8:7 10:23,24 12:23 23:12 40:5 46:23,24 48:25 71:20,24 77:4
states 24:16 58:9 68:3,14 76:11	subject 24:2 26:3,4 64:4		times 47:10 66:15
stating 69:4	submit 55:7		titled 75:7
Stephens 6:10,21 7:1 10:18,25 11:2,4 12:19 24:4 27:1 33:17 37:6 40:3,9,12,15 41:18 43:10 46:18 49:15,20,23 59:14 70:7 71:14,21 72:1,5,7 74:22 77:23 78:15 79:1,4,5,9,	submitted 7:10,21,24 8:3,7,10 49:10		today 6:17 7:7,9 8:8,9,21 9:25 26:13 72:9
	subsection 19:13 24:6,16 66:22 67:1,24 69:10		today's 7:3 9:8
	substance 72:8		tokens 51:15
	suggested 32:23		tool 75:10
	support 29:13		transcript
	sworn		
		T	
		taking 21:13,21	
		talk 17:2	
		talking 20:5 24:3 30:24 58:17 76:23 77:11,20	
		talks 24:13	
		Tamara 6:3 49:15	
		technical 12:22 62:25	
		techniques 32:24 36:23 57:24	
		telling 30:22	
		tells 30:24	
		templates 9:2	
		term 31:16	
		terms 30:5 51:21	

Index: speaking-transcript

THE SULLIVAN GROUP OF COURT REPORTERS

79:2	52:10 55:8 59:5		
transformed 13:14	understanding 14:3,18 19:24 21:10 22:12 25:8 30:18 50:25 65:18	W	Z
true 7:22 71:2 75:10,12,23 77:19 78:14	understood 19:25 25:23 39:13	wanted 37:3	zip 10:7,8,13 20:12 21:19 49:18
trusted 17:24 18:6 24:14 29:6 35:21 36:2,5 40:23 45:6,10	unique 34:7	warehouse 11:13 38:25 39:5,10,17 46:7,20 48:11,13,18 49:1 50:1,10,20 51:6,8, 11,16,24 53:6 54:20,23 55:22 56:16 57:2,4,11 58:2	
truth 6:7,8	uniquely 34:22 37:12	wasteful 50:16	
truthfully 7:6	Unlike 11:11	ways 15:8,9,12 16:15 17:4,25 29:1,18 30:22 62:16	
turn 12:20 20:24 31:13,20 37:25 44:11 58:5 63:10 66:21 69:16 72:12 74:23	unquote 58:11	wider 76:12	
turning 16:20	update 50:10	word 60:19	
two-fish 33:14	usefulness 22:3	work 40:6 48:3 52:11	
type 12:24	user 38:4,5,12 74:15 75:22 77:6	works 75:9	
types 11:11 47:4	users 76:3	worried 43:22 56:22	
	V	worse 12:24	
U	values 76:13	wrap 71:17	
U.S. 13:6	vary 39:15	write 9:2	
unable 20:16 33:11,25 34:2	Venable 6:24	writing 8:25	
unauthorized 33:2	verify 68:20	writings 9:18	
unavailable 29:6,9,11	view 23:20 27:15 52:22	written 8:17	
unaware 22:21	Vigilytics 6:18	Y	
unclear 30:21	violate 58:24 71:8	years' 29:16	
understand 6:19 7:2,9,13 8:12 14:5 16:21 20:6 28:22 30:19 31:17 37:18 39:18 41:21 47:22 48:2,14	violation 41:9 52:20,23 53:1,18 55:11,13 56:23	yield 16:13 22:4	
	violations 53:21 56:1		

Index: transformed-zip