

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

4 DATAVANT, INC.,

5 Petitioner,

CERTIFIED COPY

6 v.
7

8 VIGILYTICS LLC,

9 Patent Owner.
10

11 Cases:

11 IPR2024-00307 (US Patent No. 9,965,651)
12 IPR2024-00311 (US Patent No. 10,109,375)
13 IPR2024-00381 (US Patent No. 10,886,012)
14 IPR2024-00382 (US Patent No. 9,665,685)
15

16 VIDEOCONFERENCE DEPOSITION OF

17 DR. PAUL CLARK

18 MARCH 20, 2025

19 Page 1 - 81

20 10:09 a.m. - 1:22 p.m. EST

21 REPORTED BY:

22 Tamara L. Houston

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

24 Job Number: J12600076

25 Ref. 25412-0021IP1

Ref. 25412-0024IP1

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 10:09 a.m. to 1:22 p.m. EST, Thursday, March 20,
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.**
6 **600 Massachusetts Avenue, NW**
7 **Washington, DC 20001**
8 **(202) 721-5423**
9 **joliver@venable.com**

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

11 **FISH & RICHARDSON, P.C.**
12 **BY: NICHOLAS STEPHENS, ESQ.**
13 **3200 RBC Plaza**
14 **60 South Sixth Street**
15 **Minneapolis, Minnesota 55402**
16 **(612) 335-5070**

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

MARCH 20, 2025

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

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

--o0o--

(Exhibits marked electronically.)

1 Thursday, March 20, 2025, 2025, 10:09 a.m.

2 --000--

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

5 --000--

6 DR. PAUL CLARK,
7 called as a witness

8 was sworn and testified as follows:

9 --000--

10 EXAMINATION BY MR. STEPHENS:

11 Q. Good morning, Dr. Clark.

12 A. Morning.

13 Q. I believe this is our third or fourth session
14 on these cases, so I'll try to keep the housekeeping
15 items to a minimum.

16 As you know, my name is Nick Stephens. I'll
17 be taking questions today on behalf of the patent owner
18 here, Vigilytics.

19 MR STEPHENS: Would counsel for Petitioner
20 like to make an appearance?

21 MR. OLIVER: Justin Oliver from Venable on
22 behalf of the Petitioner Datavant.

23 BY MR. STEPHENS:

24 Q. Dr. Clark, you understand that you are under
25 oath for today's deposition?

1 A. Yes.

2 Q. Is there any reason that you cannot testify
3 truthfully and completely in responding to my questions
4 today?

5 A. No.

6 Q. I'll do my best to phrase my questions
7 clearly, but undoubtedly I'll fall short at times. If
8 you ever don't understand the question or need me to
9 repeat or rephrase a question, please let me know.
10 Okay?

11 A. Yes.

12 Q. And if you don't ask me to repeat or rephrase
13 a question, I'll assume that you understood the
14 question. Is that fair?

15 A. Yes.

16 Q. I'll also need to take a short break every
17 hour or so, and we'll -- we can further plan for a
18 longer lunch break. If you ever need to take a break as
19 well, just let me know. Okay?

20 A. Yes.

21 Q. Do you understand that we're here today
22 regarding the reply declarations that you submitted in
23 the IPRs on the '651, '375, '012, and '685 patents?

24 A. I do.

25 Q. And these are the second declarations that you

1 submitted in each of these proceedings. Correct?

2 A. Second set of patents, but not the second
3 declaration.

4 Q. You submitted a first declaration in each of
5 these proceedings that was -- that accompanied the
6 petition. Correct?

7 A. Yes.

8 Q. And this reply -- the reply declarations that
9 you recently submitted, these would be the second
10 declarations in each of the proceedings?

11 A. Yes.

12 Q. For the record, the reply declarations have
13 each been marked as Exhibit 1015 in their respective
14 proceedings. And your earlier declaration was marked as
15 Exhibit 1003.

16 For simplicity, I'll focus most of my
17 questions today around the reply declarations that you
18 recently submitted and, in particular, the reply
19 declaration in the IPR in the '651 patent, which is
20 Exhibit 1015 and IPR 2024-00307. Okay?

21 A. Yes.

22 Q. When I refer to your declaration today, I'll
23 be referring to the '651 reply declaration unless I
24 indicate otherwise. Okay?

25 A. Yes.

1 Q. Dr. Clark, do you have any electronic or
2 printed written materials with you currently?

3 A. Nothing open, no.

4 Q. And as we discussed before we went on the
5 record, you have electronic copies of the number of
6 files from the records available. Correct?

7 A. Yeah, limited to one directory. I moved the
8 four reply declarations, and as I said, former exhibits,
9 1004 through 1009, which include the references in my
10 CV.

11 Q. Apart from the Zoom feed that I can see here,
12 do you have any communication channels open with counsel
13 or anyone else?

14 A. No. Let me confirm that another window
15 doesn't have email open and I'll shut it for you. No.
16 No emails. And no messaging.

17 Q. Thank you. If that changes during your
18 deposition, just let me know.

19 A. It will not.

20 Q. How did you prepare your reply declaration?

21 A. We discussed my opinions with regard to
22 proceedings at the PTAB as well as other issues, and
23 then we wrote the dec -- the replies. That was it.

24 Q. Okay. How much of the reply declarations did
25 you draft on your own as opposed to the words being

1 drafted by counsel?

2 A. As we've discussed before, I don't really keep
3 track of that. I -- I did a significant amount of work
4 drafting.

5 Q. And about how much time did you spend
6 preparing the reply declarations in these proceedings?

7 A. Several hours.

8 Q. More than five hours?

9 A. I'm sure.

10 Q. Less than 15?

11 A. I don't know for sure. I haven't checked my
12 timesheets.

13 Q. Are you aware of any errors in your
14 declarations?

15 A. No. If I was, I would have fixed them.

16 Q. And how did you prepare for today's
17 deposition?

18 A. I had a Zoom with counsel for Venable.

19 Q. When did that occur?

20 A. Yesterday.

21 Q. And about how much time did you spend
22 preparing for the deposition?

23 A. Couple hours.

24 Q. Did you independently review any materials
25 apart from your meeting with Venable?

1 A. Yes.

2 Q. Are there any materials that you reviewed that
3 are not identified in the list of materials considered
4 in your declarations?

5 A. No.

6 Q. And I understand that the opinions in your
7 declarations are offered from the perspective of a
8 person of ordinary skill in the art at the time of the
9 claimed inventions; is that correct?

10 A. Yes.

11 Q. If I use the term "POSA" or "POSITA" as a
12 shorthand for a person of ordinary skill in the art,
13 will you know what I mean?

14 A. Yes.

15 Q. All right. Great. I would like to turn to
16 several topics; but as we do, I'd ask that you answer
17 the substantive questions today from the perspective of
18 a person of skill in the art as you understand it.
19 Okay?

20 A. I'll do my best.

21 Q. All right. Let's get started.

22 So if you could open your reply declaration in
23 the '651 patent, please.

24 A. Okay.

25 Q. And turn to paragraph 7.

1 Are you there?

2 A. Okay.

3 Q. The fourth line down, the sentence that
4 begins, "I also understand that Vigilytics has generally
5 agreed with definition of a POSA in my prior
6 declaration; however, Vigilytics asserts that the POSA
7 would have had specific knowledge about medical
8 databases and the manner of operating the same to comply
9 with HIPAA."

10 Do you see that?

11 A. Yes.

12 Q. Do you recall how you defined a POSA in your
13 prior declaration?

14 A. Not from memory, no.

15 Q. And in the zip file I sent through the chat, I
16 put in a copy of your first declaration in the '651 IPR
17 proceeding.

18 Were you able to access that?

19 A. Or I can accept your representation as to
20 what's in there. It's up to you.

21 Q. If you would open that, I think that would
22 be -- I'd appreciate if you could follow along with me.

23 A. I'll try and get -- is this in the share?

24 Q. Yes.

25 A. Which button? Is that under docs or is it --

1 I don't know where that stuff shows up.

2 Q. Let me -- I'll put this individually into the
3 chat. Might be easier.

4 A. Yeah.

5 Q. Okay. Once you have it open, I'll turn to
6 paragraph 22.

7 A. Yep.

8 Q. This is where you set forth the definition for
9 a POSA of the '651 patent.

10 A. Yes.

11 Q. And do you still stand by this definition of a
12 POSA?

13 A. Sure. It's not, as I said, significantly
14 different of the ones you guys have used.

15 Q. In the -- turn to paragraph 34 in this
16 declaration, which is the background '651 patent.

17 A. Okay.

18 Q. And the first two sentences you wrote that,
19 "The '651 patent relates to a computer-implemented
20 system of producing information characterizing a group
21 of individuals from a set of private data representing
22 characteristics of individuals. De-identification is
23 done in order to comply with the Health Insurance
24 Portability and Accountability Act, HIPAA."

25 Do you see that?

1 A. That's what it says.

2 Q. And you stand by the accuracy of this
3 explanation. Correct?

4 A. Yes.

5 Q. So the '651 patent is concerned with HIPAA
6 compliance. Correct?

7 A. Among other things, yes.

8 Q. And the other four Vigilytics -- the other
9 four patents at issue are similarly concerned with HIPAA
10 compliance. Correct?

11 A. Yes, among other things.

12 Q. Why would a POSA implementing a medical
13 records database be concerned with HIPAA compliance?

14 A. Because that's what governs the healthcare
15 providers that they would be implementing systems for.

16 Q. A POSA would have been aware of penalties
17 imposed by law for violating the HIPAA Privacy Rule.
18 Correct?

19 A. I doubt that. They would have just seen them
20 as system requirements for implementation.

21 Q. Are you aware of any penalties that could be
22 incurred for knowingly implementing a system that
23 violated HIPAA?

24 A. I'm not a lawyer. I would say that there
25 would certainly -- if you were negligent, there would be

1 civil liability.

2 Q. Are you aware of any criminal liability for
3 knowingly violating HIPAA?

4 A. I'm not familiar with the law, no.

5 Q. Let's assume for a moment that HIPAA does
6 impose civil and criminal penalties for known violations
7 of the privacy rule. Okay?

8 A. That's fine.

9 Q. In that case, would a POSA have been motivated
10 to implement a system that handles protected health
11 information but fails to comply with HIPAA?

12 A. A POSA would have implemented the system
13 according to requirements, and so the HIPAA requirements
14 with regard to data security would have been outlined
15 with regard to de-identification and disclosure of PII,
16 and so they would have been motivated to implement a
17 system that complied with those requirements. But I
18 don't think they would have necessarily been concerned
19 with civil or criminal liability, no.

20 Q. If a POSA knew that they would face -- that
21 they could face civil or criminal liability for
22 knowingly implementing a system that violated HIPAA,
23 would they, nonetheless, proceed down that path?

24 A. A POSA would, as I said, implement a system
25 according to system requirements, period. That's how

1 tech -- technologists work. They -- I mean, you always
2 work under the threat of liability for disclosures and
3 other things, but the system would be implemented
4 according to the requirements that they were given,
5 period.

6 Q. Are the system -- when you say system
7 requirements, would that also include -- would that
8 encompass requirements for regulatory compliance?

9 A. The requirements would have been to -- a
10 person at that level of skill would have been given that
11 you had to de-identify and use reasonable
12 countermeasures to make sure that personally
13 identifiable information was not disclosed. Those would
14 have been the requirements.

15 Q. And would reasonable -- would reasonable
16 countermeasures need to comply with HIPAA?

17 A. The reasonable countermeasures would be aimed
18 at complying with HIPAA, but the technologist would be
19 given system and technical requirements. They wouldn't
20 hand them the HIPAA regulations and say, "Implement
21 something that looks like this." That's not how it
22 works.

23 Q. Would you agree that a POSA is more than just
24 a technologist who is charged -- tasked with
25 implementing a system that's been provided to them by a

1 set of design requirements?

2 MR. OLIVER: Objection. Form.

3 THE WITNESS: No. The POSA would have been
4 familiar with requirements that would come from HIPAA,
5 but the -- the system requirements, they would define
6 from there, which is de-identification and don't
7 disclose PII, and those would have been the
8 requirements.

9 BY MR. STEPHENS:

10 Q. If a POSA were designing a system that handled
11 protected health information, would they have been
12 motivated to comply with HIPAA?

13 A. They would have been motivated to employ
14 countermeasures that provided for de-identification and
15 protection of PII.

16 Q. And those are requirements under HIPAA.
17 Correct?

18 A. Yes.

19 Q. All right. I'll now refer to the '651 patent
20 itself, which is Exhibit 1001 in the '651 proceeding.

21 Do you have a copy of that patent?

22 A. I don't. I do, but I don't want to go looking
23 for it on you.

24 Q. I can put it quickly in the chat.

25 A. Yep.

1 Q. All right. Turn to Figure 2, please, of the
2 '651 patent.

3 A. Okay.

4 Q. And at the right side of Figure 2, there is a
5 user or indicator of the hospital 150.

6 Do you see that?

7 A. Yes.

8 Q. Fair to say there's a beta flow that loops
9 from the user through a third party 205, through a data
10 aggregator 206; then through a data processor 210, and
11 then back to the hospital 150.

12 Do you see that?

13 A. Well, I was on actually the wrong figure.

14 Q. I'm on Figure 2.

15 A. Yeah, I was cleverly on Figure 1. Let's
16 see -- yes, I see that.

17 Q. So the hospital 150 sent a data request 203 to
18 a third party 205. Correct?

19 A. Yep.

20 Q. What would be included in that data request
21 203?

22 A. I don't know. Well, anything.

23 Q. But I guess, based on your understanding of
24 the '651 patent, what would be included in the data
25 request?

1 A. It would be a request for a healthcare record.

2 Q. And are you familiar with what data would be
3 included in the request?

4 A. I -- it could be any number of things.

5 Q. Such as?

6 A. I didn't hear your question.

7 Q. I'm sorry. You said it could be any number of
8 things, and I was asking, "Such as?" Can you provide an
9 example?

10 A. Yeah. Maybe a previous health condition,
11 maybe, you know, current allergies. I mean, I don't
12 know. Any -- anything.

13 Q. And sitting here right now, do you recall what
14 the '651 patent describes with respect to the data
15 request?

16 A. Not from memory, no.

17 Q. Would the data request include a request for a
18 group of individuals -- a request for healthcare
19 information with respect to a group of individuals?

20 A. Certainly could.

21 Q. And how would the individual be identified in
22 the data request?

23 A. I would have to look to the patent to see what
24 examples they give. But, again, it could be any number
25 of things.

1 Q. Okay. So the data request 203 is received by
2 a third party 205. Correct?

3 A. Yes.

4 Q. And what does the third party 205 then do with
5 that data request?

6 A. Sends it to a data aggregator.

7 Q. Does it perform any processing on the data
8 request before sending to the data aggregator?

9 A. Since it's sending tokens, according to this
10 embodiment, which is what the figure indicates, it would
11 have de-identified that data request.

12 Q. And can you explain what you mean by
13 de-identified the data request?

14 A. Yeah. It would have removed the PII from the
15 data request.

16 Q. That's how the '651 patent describes creating
17 request tokens by de-identification?

18 A. I believe so. I can look in the patent and
19 see what else it says, if you wish.

20 Q. So the request token 204 is received by the
21 data aggregator 206. Correct?

22 A. In this embodiment, yes.

23 Q. And what's -- what is the function -- strike
24 that.

25 What does the data aggregator 206 do with the

1 request tokens?

2 A. Looks like it sends them to a data processor
3 to be included in the report.

4 Q. Sends the request tokens through the data
5 processor 210?

6 A. That's what the figure shows.

7 Q. Do you recall anything else that the data
8 aggregator 206 does with the request tokens?

9 A. Well, it would have to issue a -- though it's
10 not shown in the figure, it would have to issue a query
11 to the remote sites shown as claims, clearing houses,
12 and pharmacies and the like.

13 Q. And what would that -- strike that.

14 The data processor 210 then receives requested
15 de-identified data 208 from the data aggregator 206.
16 Correct?

17 A. That's what -- in this embodiment, that's what
18 it shows, yes.

19 Q. And finally, the data processor sends a report
20 212 back to the hospital 150. Correct?

21 A. That's what Figure 2 shows.

22 Q. What's the difference -- we see the request of
23 de-identified data 208 that's sent to the data processor
24 210. Correct?

25 A. Yes.

1 Q. And then the data processor provides a report
2 212 to the hospital 150 as we just discussed. Correct?

3 A. In this embodiment, that's what it shows, yes.

4 Q. And is there a difference between the request
5 of the de-identified data 208 and the report 212?

6 A. If it goes through a data processor, I would
7 assume so.

8 Q. Based on your understanding, what would be the
9 difference between those two?

10 A. Guessing at least formatting to generate the
11 report, but any number of things could change depending
12 upon the way you implement the system.

13 Q. Let's turn to Column 5 at line 34.

14 If you would like to take a moment to review
15 that paragraph, please feel free.

16 A. Yes, I see.

17 Q. That line, 34 through 37, the patent explains
18 that, "De-Identified data records may be provided to the
19 data processor 210 (e.g., a third-party data processor),
20 but that third party may not have access to any
21 personally identifiable information 118 about the group
22 154."

23 Correct?

24 A. That's what it says.

25 Q. And then the last sentence of that paragraph

1 explains that "These features of the system 200 maintain
2 the privacy of the protected health information 130."

3 Correct?

4 A. That's what it says.

5 Q. Why is it important that that third-party data
6 processor not have access to the, quote, "requested
7 de-identified data 208 and the personally identifiable
8 information 118 about the individuals in the group"?

9 MR. OLIVER: Objection. Form. Foundation.

10 THE WITNESS: In this embodiment, it seems
11 that that data processor is not intended to be a covered
12 business entity, so it can't have access to the PII.

13 BY MR. STEPHENS:

14 Q. There would have been a re-identification risk
15 then if the data processors had access to both the
16 de-identified data records and the PII. Correct?

17 A. Not necessarily. Depends on how it was
18 implemented.

19 Q. Well, why did the patent explain again that
20 the third-party data processor may not have access to
21 both the de-identified data records and the PII?

22 A. As I already explained, in this embodiment the
23 data processor is not anticipated to be a covered
24 business entity, so it's not allowed to have access to
25 the PII.

1 Q. Is there a provision in here that you're
2 referring to that would preclude a --

3 (Interruption.)

4 A. Sorry, home pod. I just unplugged it.
5 Can you please re-ask the question?

6 Q. Yeah, I'll rephrase my question.
7 Are you -- are you familiar with the
8 difference between PII and PHI?

9 A. Yeah, one is healthcentric, and the other is
10 just personally identifiable.

11 Q. So PII is personally identifying information.
12 Correct?

13 A. Yes.

14 Q. And PHI refers to protected health
15 information. Correct?

16 A. That's correct. They overlap.

17 Q. The term -- does the term "protected health
18 information" have a defined meaning under HIPAA?

19 A. Yes.

20 Q. And what is that?

21 A. I'm not going to work from memory. I mean, if
22 you want to bring up the standard, we can look at them.

23 Q. All right. Let's take a look. I'll put it in
24 the chat, Exhibit 2006.

25 A. All right.

1 Q. And so at the top of the first page, you see
2 this line that reads, "Section 164.514, other
3 requirements relating to uses and disclosures of
4 protected health information"?

5 A. Yes.

6 Q. And so this is -- this, by the way, is the
7 text of the HIPAA Privacy Rule. Correct?

8 A. I don't see a heading -- oh, I see it. Yes,
9 that's what it says.

10 Q. So the HIPAA Privacy Rule governs uses and
11 disclosures of protected health information. Correct?

12 A. Yes.

13 Q. Does the HIPAA Privacy Rule -- strike that.

14 Using this to refresh your memory, can you
15 explain, again, the distinction between protected health
16 information and personally identified information?

17 A. Yes. The PHI, according to this, is broader;
18 but as I said, they overlap.

19 Q. Does HIPAA govern the use and disclosure of
20 PII that is not PHI?

21 A. I am having trouble thinking of anything that
22 is PII that is not PHI.

23 Q. So can you think of -- I guess if you need to
24 take a moment, please do -- but can you think of any
25 examples of PII that would not be PHI?

1 A. That's what I said. I'm having trouble coming
2 up with any. This would identify a patient that would
3 not then be covered under PHI.

4 Q. I've put into the chat Exhibit 1016.

5 A. Can I close the other HIPAA one?

6 Q. Yes, you may.

7 A. Okay. Got it.

8 Q. You cited Exhibit 1016 in your reply
9 declarations. Correct?

10 A. I believe that's true.

11 Q. What is Exhibit 1016?

12 A. Guidance -- HIPAA guidance from HHS.

13 Q. Turn to page 5.

14 A. Okay.

15 Q. And will you please read the paragraph that
16 begins -- the last paragraph that begins with, "The
17 relationship with health information is fundamental."

18 A. I see what it says.

19 Q. So, again, can you think of any examples of
20 PII that would not constitute PHI?

21 A. No, I disagree with their characterization.
22 If I can identify a patient's name or Social Security
23 number, the name being -- or phone number being in a
24 phonebook, this still would need to be de-identified as
25 it relates to a health record.

1 So their guidance is flawed.

2 Q. In your view, the guidance in Exhibit 1016 is
3 flawed?

4 A. Yes, because it -- again, if I have such
5 information with health information, you don't want to
6 be able to identify the names or addresses or phone
7 numbers of patients. So it would need to be
8 de-identified as far as de-identifying the health
9 record.

10 Q. So this would not be a reliable evidence to
11 rely upon?

12 A. I didn't say that. I just said I disagree
13 with the characterization here. I think it's
14 incomplete.

15 Q. No. You said it was flawed. Correct?

16 A. Because it's incomplete.

17 Q. Okay. Let's turn back to the '651 patent,
18 please.

19 A. Okay.

20 Q. And we were looking at the disclosure at
21 Column 5, lines 34 to 42.

22 Do you recall that?

23 A. Yes.

24 Q. And the data -- again, it says that the data
25 processor -- excuse me, "De-Identified data records may

1 be provided to the data processor 210 (e.g., a
2 third-party data processor) but that third party may not
3 have access to any personally identifiable information
4 118 about the group 154."

5 Correct?

6 A. That's what it says.

7 Q. Would -- now, the de-identified data records
8 that are provided to the data processor, they -- those
9 are records of the -- those are de-identified data
10 records of the individuals in the group 154. Correct?

11 A. In this embodiment, yes.

12 Q. And so would having the PII for those
13 individuals increase the likelihood that the data
14 processor 210 could re-identify the patients that could
15 also have the de-identified records?

16 MR. OLIVER: Objection. Form.

17 THE WITNESS: Yeah. I don't have enough
18 information to know.

19 BY MR. STEPHENS:

20 Q. Well, are you familiar with the concept of the
21 re-identification risk, Dr. Clark?

22 A. Yes.

23 Q. And what is the re-identification risk?

24 A. The idea that you can identify the individual
25 from the token.

1 Q. From what token?

2 A. From the de-identification token.

3 Q. From the de-identified data records?

4 A. Which are identified by tokens.

5 Q. Okay. So the data processor 210 received the
6 de-identified data records for the individuals in the
7 group. Correct?

8 A. Yes.

9 Q. And statistically, there's some possibility of
10 re-identification from the de-identified data records.
11 Correct?

12 A. No. Not statistically. It depends upon how
13 the system is implemented.

14 Q. If you knew the individuals -- the identities
15 of the individuals in the group -- I'll rephrase this.

16 Is it your testimony, just sitting here today,
17 that the '651 patent was not concerned with the
18 re-identification risk if the data processor were to
19 receive the PII and the de-identified data records?

20 MR. OLIVER: Objection. Form.

21 THE WITNESS: That's ridiculous.

22 BY MR. STEPHENS:

23 Q. Well, I asked you earlier -- I asked what was
24 the risk, and you said there was no re-identification
25 risk.

1 A. I didn't say there was no re-identification
2 risk. I never uttered those words.

3 Q. So why, again, then does the patent not allow
4 the data processor to patent -- to have access to both
5 the de-identified records and the PII.

6 A. Because it's not a covered business entity. I
7 answered that question a half hour ago.

8 Q. Would it be covered by HIPAA? Or would it be
9 a covered entity if it received both the de-identified
10 records and the PII?

11 A. If it wanted to be compliant, it would have --
12 there would have to be an agreement in place, or it
13 would have to be a covered entity according to HIPAA.

14 Q. If the third-party possessed both the
15 de-identified data and the names of the individuals in
16 the group, how does re-identification occur?

17 A. If I have your name and I have a health
18 condition, it's possible that I could, depending upon
19 whether they are using pseudonyms or not or whether the
20 name was Joe Smith, that I may or may not be able to
21 re-identify you, but I would not implement a system in
22 which the patient's names were available. That's for
23 sure.

24 Q. And why would you not do that?

25 A. Because I would not want someone with a unique

1 name to have their name out there with a health
2 condition that then would allow me to infer the
3 protected health information. That would not be
4 prudent.

5 Q. That would be a re-identification risk?

6 A. I think it could be. I mean, I -- I wouldn't
7 recommend anyone to do that.

8 Q. You wouldn't recommend anyone to provide both
9 the de-identified data records and the names of the
10 individuals?

11 A. I would not recommend that you include names
12 in de-identified data, whether or not it was compliant
13 or not.

14 Q. Right. So you wouldn't -- you would not
15 provide the names and the de-identified records to the
16 same entity. Correct?

17 MR. OLIVER: Objection. Mischaracterizes.

18 THE WITNESS: Right. I would not have names
19 and health conditions available to someone that was not
20 a covered entity. That wouldn't be the way I would
21 implement the system.

22 BY MR. STEPHENS:

23 Q. Because there's a risk of breaching the
24 patient's privacy. Correct?

25 A. In my opinion, there would be a risk.

1 Q. And based on the disclosure at 34 -- I'm
2 sorry, Column 5, lines 34 to 42, the '651 patent
3 recognizes that risk as well. Correct?

4 A. I don't know. It doesn't talk specifically --
5 let's see (speakign sotto voce.) Well, that's what he
6 said. In general, PII is a subset of PHI. So right,
7 you would not want the names available according to the
8 '651 in this embodiment.

9 Q. Let's turn to Column 8, please.

10 A. Okay.

11 Q. And I'll look at the paragraph that begins at
12 line 35 through line 46, if you'd like to take a moment.

13 A. Okay.

14 Q. And so at lines 39 through 41, the patent
15 explains that, quote, "Individual tokens are placed in a
16 batch file and may be encrypted before being transmitted
17 over the network," correct?

18 A. Yes. This is for the embodiment described in
19 Figure 5, but that's what it says.

20 Q. What is a batch file?

21 A. A batch file is usually a group of operations
22 defined and stored within a file that are then executed.

23 Q. And in the context of a '651 patent, the batch
24 file is a file -- well, I'll ask if this is correct.

25 Is a batch file a file that contains the

1 individual tokens?

2 A. According to the '651, a batch file is a term
3 of art that's intended to be executed on a processor
4 with a series of operations usually at a specified time,
5 in fact; but in this case, according to the '651, it's
6 talking about encrypting tokens that are part of a batch
7 file.

8 Q. So the patent encrypts the PII to create the
9 request tokens. Correct?

10 A. It describes encrypting the batch file before
11 it's transmitted over the network.

12 Q. Okay. So the batch file is encrypted -- I'm
13 sorry, the tokens are produced before creating the batch
14 file. Correct?

15 A. That's what it says.

16 Q. And then the batch file is encrypted before
17 being transmitted over the network. Correct?

18 A. In this embodiment, that's what it says.

19 Q. And then the de-identified data server then
20 decrypts the batch file to recover the tokens and use
21 its roles for searching, matching, and retrieving
22 healthcare data. Correct?

23 A. In this embodiment, that's what it says, yes.

24 Q. When it decrypts the batch file, then it
25 recovers the tokens. Correct?

1 A. That's the way it's described, yes.

2 MR. STEPHENS: We've been going for about an
3 hour. Can we take a ten-minute break?

4 THE WITNESS: That's fine.

5 MR. OLIVER: Okay.

6 MR. STEPHENS: Okay. Back at 11:20 Eastern.

7 (Recess: 11:09 a.m. to 11:24 a.m., EST.)

8 BY MR. STEPHENS:

9 Q. Dr. Clark, I'd like to stick with the '651
10 patent and turn to Claim 1, please.

11 A. Okay.

12 Q. So Claim 1 refers to a computer-implemented
13 method comprising receiving a request from a user device
14 for information that characterizes a group composed of
15 multiple individuals from a set of de-identified medical
16 data representing characteristics of the individuals'
17 pre- or post-encounter with a healthcare facility."

18 Did I read that correctly?

19 A. Yes.

20 Q. What does the term "pre- or post-encounter
21 with a healthcare facility" refer to?

22 A. It says plain English meaning.

23 Q. And the '651 patent describes techniques for
24 performing pre- or post-encounter analyses. Correct?

25 A. I believe so.

1 Q. Are the terms "pre- and post-encounter" terms
2 of art in the '651 patent?

3 A. As I said, plain English meaning.

4 Q. Turn to Column 6, please.

5 A. Okay.

6 Q. I'll look at a paragraph that begins at line 6
7 through line 28.

8 A. Okay.

9 Q. And this paragraph refers to a request message
10 306. Correct?

11 A. Yes.

12 Q. The request message can include identifying
13 data 404 for a group of individuals. Correct?

14 A. That's what it says.

15 Q. And then there is also nonidentified data 405
16 associated with the request message 306. Correct?

17 A. Yes.

18 Q. And at nine, identified data 405 is for
19 pre-encounter and/or post-encounter details such as
20 service dates or diagnosis information. Correct?

21 A. That's what it says.

22 Q. What would a POSITA understand a service date
23 to be?

24 A. Plain English, the date of service.

25 Q. Of what service?

1 A. Healthcare service.

2 Q. Could it be a discharge date?

3 A. Any date associated with healthcare, I would
4 think.

5 Q. Likewise, how would a POSITA understand -- or
6 what would a POSITA understand diagnosis information to
7 be?

8 A. Plain English meaning.

9 Q. And a service date and diagnosis information
10 from the medical record would be protected health
11 information under HIPAA. Correct?

12 A. I would have to look at the standard, but I
13 would think so.

14 Q. As described in this paragraph, the service
15 date for diagnosis information are separated from the
16 PII 404 to create nonidentified data 405. Correct?

17 A. In this embodiment, yes.

18 Q. And the patent explains that access to the
19 service date or nonidentified data 405 is restricted
20 only to the report generator 328. Correct?

21 A. That's what it says.

22 Q. Why does the patent implement measures to
23 restrict access to the service date or the nonidentified
24 data, only to the report generator?

25 A. I don't know. I don't have it memorized, the

1 patent, where it may or may not explain that.

2 Q. Based on your understanding or based on the --
3 would a POSITA have understood reading the patent why
4 that would be?

5 A. A person who understands security would
6 understand the concept of least privilege which means if
7 you don't have to make information available, then you
8 should not. It's a default/deny model.

9 Q. And from a HIPAA perspective, is there any
10 reason why a POSA would not provide the service date or
11 diagnosis information along with the PII?

12 A. I have not memorized the standard, so I don't
13 know the answer to that from memory.

14 Q. Do you have an understanding of what the
15 service date would be used for in a pre- and
16 post-encounter analysis?

17 A. I mean, I'm not a doctor, but I could guess.

18 Q. Well, in the '651 patent, how would you?

19 A. I don't know. I don't have total recall of
20 the '651 patent. I know what the plain English meaning
21 of service date is. I could guess why it would be
22 useful to a doctor. That's all.

23 Q. Why do you believe it would be useful in a
24 pre- or post-encounter analysis?

25 A. Recency of different treatments or symptoms,

1 it is useful information.

2 Q. Would a pre- and post-encounter analysis
3 require an index date from which to measure the date of
4 the encounter with the healthcare facility?

5 A. I don't know; I'm not a doctor.

6 Q. Do you believe you need to be a doctor to
7 understand a pre- or post-encounter analysis?

8 A. That's not what I said, and that was not your
9 question.

10 Q. I'm asking a separate question. I'm following
11 up on your response to my last question. You said, "I
12 don't know because I'm not a doctor." So I asked
13 whether you need to be a doctor to understand a pre- or
14 post-encounter analysis.

15 A. I understand what a pre- and post-encounter
16 analysis is.

17 Q. And what is it?

18 A. Plain English meaning.

19 Are you sitting there just trying to waste
20 time, Counselor? I mean, I don't get this.

21 Q. Well, when you say a "plain English meaning,"
22 that doesn't shed any light to --

23 A. This is not a subject of my declarations. It
24 looks to me like you're simply trying to waste time, and
25 asking me for definitions of plain English terms is not

1 useful or informative to the PTAB or anyone else. This
2 is ridiculous.

3 Q. Dr. Clark, we're almost through this. I'd
4 appreciate your patience here. I am just trying to
5 follow up to get clarity on your response.

6 You said that a POSITA would understand the
7 pre- or post-encounter analysis, and you offered that
8 the plain English interpretation should apply.

9 I'm just asking, can you provide a little bit
10 more detail as to what the plain English meaning would
11 be?

12 A. I -- I can tell you what I would understand a
13 pre- or post-encounter analysis to be. Would be that
14 before I saw the patient I might have an idea of what
15 the symptoms imply, and then after the encounter and
16 tests or whatever treatment occurs, then I might have
17 another analysis. Plain English meaning.

18 Q. Have you ever implemented a system that
19 performed a pre- or post-encounter analysis?

20 A. I mean, I've implemented expert systems
21 before, but I don't believe I implemented an expert
22 system in healthcare, no.

23 Q. What is an expert system? Can you explain to
24 me what that means?

25 A. An expert system does analysis based upon

1 rules and knowledge. It's a knowledge-based system.
2 That's how you would perform an analysis.

3 Again, this is not the subject of any of my
4 declarations, and it looks to me like you're simply
5 wasting time.

6 Q. You just state that, "I don't believe I
7 implemented an expert system in healthcare"; is that
8 correct?

9 A. That's correct. I've implemented other expert
10 systems but not one specifically that does medical
11 diagnoses.

12 Q. Okay. Let's turn to Column 9, please. And
13 I'll look at the paragraph that begins at line 3 through
14 line 20.

15 A. Yes.

16 Q. Okay. And at line 5 there's the sentence that
17 reads, "For example, a rule may not allow the same user
18 302 to submit more than one request message 306
19 continuing substantially the same identifying data 404
20 within a defined period of time; e.g., six months."
21 Correct?

22 A. That's what it says.

23 Q. Similar features are cited in Claim 1.
24 Correct? For reference, I'm looking at Column 12, lines
25 34 to 35.

1 A. Yes.

2 Q. And this limitation in Claim 1 refers to "a
3 privacy-preserving rule that disallows same individuals
4 to be included within a defined period of time."
5 Correct?

6 A. Yeah, it's a security concept called
7 threshold, and we've discussed in previous encounters.

8 Q. For the record, could you explain what
9 thresholding is?

10 A. Yeah, thresholding is where the system has a
11 threshold dealing with granularity usually, and also
12 period -- frequency or granularity that the system
13 limits in order to prevent inference of information.

14 Q. So when we think about a rule that disallows
15 same individuals from being included within a defined
16 period of time, would such a rule help to preserve
17 individual's privacy?

18 A. It may or it may not; but it certainly -- for
19 large-scale systems where you're seeking to prevent
20 inference from additional information, then you would
21 want to limit the frequency, as I said, or the number of
22 responses in order to prevent such inference.

23 Q. So the probability of inferring the identity
24 of an individual would increase the more time that
25 individual appears in response. Is that correct?

1 A. Not necessarily, no. But it could pose a
2 threat depending upon the types of data that are being
3 returned, and so you would want to prevent that in the
4 same way that if you have some number of failed password
5 attempts in the same period of time, you would stop
6 logins to that account, again, for some period of time
7 to prevent them from guessing the password.

8 So you don't want an attacker to be able to
9 infer anything just by repeated queries.

10 Q. Going back to Column 9, the paragraph we were
11 just looking at, at line 14, there is an example
12 provided in which the system checks that "the
13 identifying data 404 for at least five patients does not
14 match the identifying data 404 for any previous search
15 requests 306 by the user 302."

16 Do you see that?

17 A. I do.

18 Q. In this example then, the privacy-preserving
19 rule would be invoked if at least five patients
20 identified based on the first search request were
21 previously identified by the earlier request for the
22 same user within a defined period of time?

23 A. Correct. Yes. Again, preventing the
24 inference problem.

25 Q. And this analysis would involve a comparison

1 of the individuals identified by each search request.

2 Correct?

3 A. Yeah. Requires auditing of previous searches
4 so that you can compare the previous searches to the
5 current one.

6 Q. And you compare the individuals in each
7 identified search request?

8 A. In this example, yes.

9 Q. I'll take an example. If an earlier request
10 identified 500 individuals and the later request
11 identified 700 individuals, five of whom were also
12 identified by the earlier request, then the privacy rule
13 would be invoked. Correct?

14 A. Maybe, maybe not. Depends on how it's
15 implemented.

16 Q. In this example where the system is looking
17 for at least five patients that do not match the
18 identifying data from the previous request.

19 A. Yeah. If we read it literally, which says,
20 "any previous search request," then this rule would be
21 invoked. An example that involves hundreds of users,
22 I'm not sure that's the way I would implement the rule,
23 but in this example that's correct.

24 Q. The rule isn't just looking at the total
25 number of individuals identified by the request.

1 Correct?

2 A. In this example it's possible, but they are
3 interested in whether any subset matches, which is the
4 way I read this example.

5 Q. So the rule could be invoked regardless of
6 whether the total number of individuals in the earlier
7 request and the total number of individuals in the later
8 request were the same or different. Correct?

9 MR. OLIVER: Objection.

10 THE WITNESS: If that was the system
11 requirement, you could certainly do it.

12 BY MR. STEPHENS:

13 Q. But merely identifying the total number of
14 individuals identified by each request wouldn't allow
15 you to check whether the identities of the individuals
16 in each request were the same. Correct?

17 A. No. You would have to keep track of previous
18 requests, as I've said.

19 Q. Where you compared the identities of the
20 individuals in each request?

21 A. You would -- yes, you would have to keep track
22 of previous requests from this user in order to invoke
23 this rule.

24 Q. All right. Let's turn to Figure 3, please.

25 A. Okay.

1 Q. And in this figure we see a user device 302
2 that transmits a request message 306 to an encryption
3 server 312. Correct?

4 A. Yes.

5 Q. Would you agree that the request message 306
6 can be encrypted during transmission?

7 A. Yeah. You can encrypt -- for the tokens, you
8 can -- and probably would -- encrypt the channel, if
9 that's an untrusted network.

10 Q. And Column 7 at lines 34 to 37 confirms that
11 the request message 306 can be encrypted during
12 transmission. Correct?

13 MR. OLIVER: Objection. Form.

14 THE WITNESS: That's what it says.

15 BY MR. STEPHENS:

16 Q. And then if we'll look at Column 6 at lines 6
17 through 13, the patent explains that the request message
18 306 contains a set of identifying data 404 for each
19 group member; that identifying data 404 may include
20 first name, last name, date of birth, gender, zip code,
21 as well as other identifiers. Correct?

22 A. Yeah. Those are examples of PIIs we discussed
23 earlier.

24 Q. And when the request message 306 is encrypted,
25 it contains the personally identifying information

1 although in encrypted form. Correct?

2 A. Depending on how it's implemented. If -- I
3 mean, it doesn't -- I don't have enough information to
4 say there, but I would assume that that information
5 would be encrypted before it was transmitted. It might
6 also be included in the token.

7 Q. And the request message 306 is sent to the
8 token generator for the encryption server. Correct?

9 A. That's correct.

10 Q. So the request message 306 is the same request
11 token 304. Correct?

12 A. According to this embodiment, it is, yes.

13 Q. And the request message 306, again, queries
14 the PII for the individuals in the group. Correct?

15 A. In this embodiment, yes.

16 Q. And the PII is attainable from the encrypted
17 request message 306 since it can be decrypted. Correct?

18 A. If it has not yet been tokenized, then it
19 would be able -- for someone with the key to be able to
20 decrypt it.

21 Q. And it is, in fact, decrypted by the
22 encryption server 312. Correct?

23 A. Maybe, maybe not. It doesn't have to be.

24 Q. Turn to Column 4, please.

25 A. Okay.

1 Q. And let's look at line 17, the sentence that
2 reads, "A de-identifier 142 can process the PHI 130 to
3 generate irreversibly de-identified data 140 by removing
4 all personally identifiable information 118 or otherwise
5 transforming the PHI 130 so that it cannot be associated
6 with a particular person."

7 Do you see that?

8 A. I do. That's what we've been discussing.

9 Q. So the identity of the individual in this
10 example would be unattainable from the irreversibly
11 de-identified data 140. Correct?

12 MR. OLIVER: Objection. Foundation.
13 Mischaracterizes.

14 THE WITNESS: I mean, that's the objective is
15 to make sure that you can't -- don't have an
16 unauthorized disclosure of the PHI.

17 BY MR. STEPHENS:

18 Q. You agree that the identity of the individual
19 is not attainable from the irreversible de-identified
20 data 140?

21 MR. OLIVER: Objection.

22 THE WITNESS: If -- if it's done properly,
23 then it would not be attainable.

24 BY MR. STEPHENS:

25 Q. You agree that the irreversibly de-identified

1 data 140 would be absent PII. Correct?

2 A. If I were implementing the system, yes. I
3 mean, I would remove the PII and tokenize it in some
4 way.

5 Q. That's what occurs when the data is
6 irreversibly de-identified. Correct?

7 A. If it's done properly, yes.

8 Q. The irreversibly de-identified data 140 can be
9 produced by caching the protected health information
10 130. Correct?

11 A. If you do it with the correct cryptographic
12 hash, it is statistically or computationally infeasible
13 to recover the information attached. That's the purpose
14 of a cryptographic caching.

15 Q. Are there any other encryption functions,
16 one-way functions, besides hashes, that could be applied
17 to produce irreversibly de-identified information?

18 A. Yes.

19 Q. Can you give me an example?

20 A. Yes. It's possible to use symmetric ciphers
21 in a way that they create irreversibly encrypted
22 information.

23 Q. How does the symmetric cipher work?

24 A. A symmetric cipher uses the same key to
25 encrypt and decrypt information.

1 Q. So in that case you could -- you could
2 reidentify the patient, correct, by decrypting the
3 output of the encryption, if you have the appropriate
4 decryption key?

5 A. It depends on how it's used. In the example
6 that we're discussing, I said it is possible to use
7 cryptographic mechanisms other than cryptographic hashes
8 to create irreversibly encrypted information. That was
9 my statement.

10 Q. So would the cryptographic cipher, the example
11 you provided earlier, would that provide irreversibly
12 de-identified information or reversibly de-identified
13 information?

14 A. I'll say it one more time for you, Counselor.
15 This is not a cryptography class.

16 It is possible to construct a one-way cipher
17 out of a symmetric cipher; and if you do that, then it
18 would perform the same function as a cryptographic hash.
19 Used in its usual way, you would encrypt and decrypt
20 using the same key.

21 Q. So when we say constructing a one-way cipher,
22 does that mean that the output of a one-way cipher could
23 not be decrypted?

24 A. That is correct.

25 Q. So excuse me, because I'm not an expert in

1 this field, but would there not be, in that example, a
2 decryption key that would be -- that could be used to
3 decrypt the output of the one-way cipher?

4 A. No.

5 MR. STEPHENS: Let's take five minutes, if
6 that works for you.

7 THE WITNESS: That's fine.

8 MR. STEPHENS: Okay. Back at 12:06 Eastern.

9 (Recess: 12:01 a.m. to 12:10 p.m., EST.)

10 BY MR. STEPHENS:

11 Q. I'll refer again to your reply declaration in
12 the '651 IPR. Please turn to paragraph 34.

13 Are you there?

14 A. Not yet.

15 Okay.

16 Q. The second sentence in paragraph 34, you
17 wrote, "Landi explicitly states that its design presents
18 'no HIPAA issues' and that its goal is HIPAA
19 compliance."

20 Correct?

21 A. That's what it says.

22 Q. Does HIPAA compliance include compliance with
23 the HIPAA Privacy Rule?

24 A. I would think so.

25 Q. Would HIPAA compliance be important for

1 consideration to a POSITA?

2 A. In this case, yes.

3 Q. Why is that?

4 A. Because it would be built into the system
5 requirements as we discussed earlier. The -- you would
6 need to de-identify the PII and/or PHI.

7 Q. I'll back up to paragraph 30 in the reply
8 declaration. In the fourth line down you write, "While
9 Dick acknowledges HIPAA restrictions and the benefits of
10 de-identification, Dick generally contemplates methods
11 and processes for the same."

12 Correct?

13 A. That's what it says.

14 Q. So Dick was also concerned with HIPAA
15 compliance?

16 A. I don't know if it explicitly, from memory
17 anyway, describes HIPAA, but it certainly contemplates
18 de-identification of data.

19 Q. If Dick's goal or one of the goals was HIPAA
20 compliance, then you'd expect the POSITA to -- or would
21 a POSITA desire to implement features that were
22 compliant with HIPAA in Dick's system?

23 A. It would -- yeah. You would be interested in
24 protecting the privacy of individuals in the database.

25 Q. And likewise, would a POSITA be interested in

1 acquiring features in Dick's system that would not
2 comply with HIPAA?

3 A. I don't think they would want to file data,
4 but they -- usually if you're building a system that is
5 interested in data privacy, then you would be
6 implementing the features required by HIPAA.

7 Q. Do you have a copy of the Landi reference?

8 A. I do.

9 Q. If you can pull that up for me, please.

10 MR. STEPHENS: For the record, this is
11 Exhibit 1008 in each of the respective proceedings.

12 THE WITNESS: Okay.

13 BY MR. STEPHENS:

14 Q. If we could turn to Column 5, lines 7 through
15 19. Take a moment to read it, please.

16 A. Okay.

17 Q. This passage describes encrypted IDs in Landi.
18 Correct?

19 A. Well, it's describing Figure 1, which is an
20 embodiment that uses a public key cipher but, yes.

21 Q. And an encrypted ID is a unique reproducible
22 encrypted version of patient identifying information.
23 Correct?

24 A. Yes.

25 Q. And that patient identifying information, some

1 of the examples given here include patient name, Social
2 Security number, and/or address. Correct?

3 A. As -- yeah, PIIs we discussed earlier.

4 Q. The Landi's encrypted ID is derived from
5 information about the individual. Correct?

6 A. In this embodiment, yes.

7 Q. Let's look at the next column, Column 6, at
8 lines 56 to 65, please.

9 A. Okay.

10 Q. And this section describes how a healthcare
11 entity that releases de-identified patient data records
12 can securely store a respective private key for purposes
13 of reidentifying patient data. Correct?

14 A. In this embodiment, yes.

15 Q. So the encrypted ID then provides the means
16 for allowing de-identified healthcare information to be
17 re-identified by the healthcare entity. Correct?

18 A. In this embodiment, someone with access to the
19 private key can re-identify it.

20 Q. We looked earlier at the privacy rule, which
21 was Exhibit 2006.

22 Do you still have a copy of that available?

23 A. No. I closed it, but I can reopen it.

24 Okay.

25 Q. Okay. And so I'll refer on page 2 to

1 subsection C, Implementation Specifications:

2 Re-identification.

3 A. Okay.

4 Q. So a system that is assigned a
5 re-identification code to allow for de-identified
6 information to be re-identified by a covered entity
7 would need to abide by the provisions in subsection C
8 for HIPAA compliance. Correct?

9 A. That's the way I understand it.

10 Q. And there are two subprovisions under
11 subsection C, correct, the derivation and security
12 requirements?

13 A. Yes.

14 Q. And what does the derivation provision under
15 subsection 1 require?

16 A. That it's not derived from information about
17 the individual, is what it says, or otherwise capable of
18 being translated so as to identify the information.

19 Q. And as we reviewed earlier, Landi's encrypted
20 ID is derived from or related to information about the
21 individual. Correct?

22 A. That's what it said.

23 Q. So Landi's encrypted ID does not comply with
24 the derivation requirement. Correct?

25 A. I'm not sure that's true because you have to

1 have access to the key in order to do it; but generally
2 speaking, in that embodiment, you could argue that it's
3 not combined with a derivation requirement.

4 Q. And, likewise, do you recall in the last
5 deposition that you testified that Landi's encrypted ID
6 would not be compliant with the derivation requirement?

7 MR. OLIVER: Objection. Foundation.

8 THE WITNESS: I don't actually remember saying
9 that, but certainly for that embodiment, the information
10 is being derived, but that doesn't mean that a POSITA
11 couldn't easily fix that, so I don't really see a
12 problem.

13 MR. STEPHENS: Can we go off the record for a
14 minute?

15 THE WITNESS: Yes.

16 (Recess: 12:24 p.m. to 12:28 a.m., EST.)

17 BY MR. STEPHENS:

18 Q. Let's turn back to Landi, please, at Column 1.
19 And under the paragraph -- the paragraph beneath the
20 section, "Technical Field of the Invention," it
21 describes what the present invention relates to.

22 Do you see that?

23 A. I don't just yet. Hold on. My screen got
24 messed up.

25 Okay. So you said Column 1.

1 Q. Column 1, line 14, under the "Technical Field
2 of the Invention."

3 A. I see it.

4 Q. In this paragraph it describes how -- "to
5 systems and methods that implement the secured key
6 encryption for de-identifying patient data to ensure
7 patient privacy, while allowing only the owners of the
8 patient data records and/or other legally empowered
9 entities to re-identify subject patients of
10 de-identified data records when needed."

11 Correct?

12 A. That's what it says.

13 Q. And to allow for re-identification, Landi uses
14 reversible encryption techniques. Correct?

15 A. In the embodiment we were discussing, it was
16 using public key, but, yes, that's -- I -- normally not
17 what you would use for a symmetric cipher would be the
18 preferred mode, but, yes.

19 Q. And Landi never describes caching PII through
20 forming encrypted ID; is that correct?

21 A. Caching? I don't have complete recollection,
22 but I can search it for hash, if you wish.

23 Q. Yes, please.

24 A. The word "hash" does not appear in Landi.

25 Q. And if the PII were hashed to form the

1 encrypted ID, then you would not be able to decrypt it.
2 Correct?

3 A. As we discussed earlier, if it was hashed
4 properly with the proper algorithm, it would be one way.

5 Q. All right. Let's turn back to paragraph 19 of
6 your '651 reply declaration.

7 A. Okay.

8 Q. The last sentence of this paragraph he states,
9 "HIPAA explicitly allows for hash functions to encrypt
10 PII for de-identification." Correct?

11 A. Yes.

12 Q. And here you cite Exhibit 1016, pages 30 to
13 31. Correct?

14 A. Yes.

15 Q. And we looked at Exhibit 1016 earlier, it
16 being the HHS guidance. Correct?

17 A. I'll accept your representation. I don't
18 remember.

19 Q. Let's turn to Exhibit 1016 again, please.

20 A. Okay.

21 Q. And let's turn to page 31, which is cited in
22 your reply dec. Correct?

23 A. Yes.

24 Q. Do you see the paragraph that begins, "In line
25 with this guidance from NIST"?

1 A. Yes.

2 Q. And this -- the second sentence in that
3 paragraph states that, "The re-identification provision
4 in Section 164.514(c) does not preclude the
5 transformation of PHI into values derived by
6 cryptographic hash functions using the expert
7 determination method, provided the keys associated with
8 such functions are not disclosed, including to the
9 recipients of the de-identified information." Correct?

10 A. Yeah. They're -- that's exactly what it says,
11 and what they are talking about is for suitable
12 implementations that the derivation requirement of HIPAA
13 doesn't have to be followed, but this is guidance from
14 HHS using NIST. So, I mean, there seem to be exceptions
15 to that derivation requirement.

16 Q. So this guidance explains -- I want to make
17 sure -- that you can apply hash function to PII to
18 create a re-identification code. Correct?

19 A. That's what it says.

20 Q. Does the guidance identify any other or any --
21 strike that.

22 Does the guidance identify any reversible
23 encryption methods that could be used?

24 A. This particular guidance doesn't, but I
25 haven't seen the guidance from NIST, which may or may

1 not allow you to use public key methods which may have
2 more bits of security than the cryptographic hash
3 functions.

4 I mean, I don't -- it seems obvious that there
5 are exceptions to the derivation requirement, a
6 cryptographic hash being one of them.

7 Q. Right. Even when using a hash function, the
8 keys associated with such function cannot be disclosed,
9 including to the recipients of the de-identified
10 information?

11 MR. OLIVER: Object. Form.

12 THE WITNESS: Well, in a public key system
13 such as Landi, you wouldn't disclose the private key to
14 the recipient. So that's why they are using a public
15 key system rather than a symmetric key system.

16 BY MR. STEPHENS:

17 Q. I'm referring to the last sentence in the
18 guidance here.

19 A. I understand what you're referring to. I'm
20 giving you a complete answer based upon the point you're
21 trying to make so that there is no ambiguity.

22 Q. And what I'm referring to, again, this
23 sentence -- I'm not referring to public private key
24 methods. I'm referring to the explanation in the last
25 two lines of this guidance that cryptographic hash

1 functions using the expert determination method can be
2 used provided that the keys associated with such
3 functions are not disclosed; is that correct?

4 A. And that also applies to public key methods
5 which -- in which the private key is not disclosed, in
6 line with that guidance.

7 Q. And are you aware of any authority that under
8 the law you can use a public key method compliant with
9 HIPAA?

10 A. In the same way that you're relying upon this
11 guidance, a person of skill could rely on this guidance
12 that says that you can comply in certain circumstances
13 as long as the key is not available, and a public key
14 system does not make the private key available to those
15 with access to the data.

16 Q. And, Dr. Clark, I just want to be clear. I'm
17 not relying on this guidance. This is Petitioner's
18 exhibit, and this is the exhibit that you cited in
19 support of your analysis in your reply declaration.
20 Correct?

21 A. It is cited, yes.

22 Q. Do you believe that this guidance is reliable?

23 A. I -- I believe that it is guidance, again,
24 that relies on multiple sources for how one of skill in
25 the art might implement these systems.

1 And so if I were implementing such a system,
2 I'd be looking at government entities like HHS and NIST
3 for guidance how to implement this.

4 Q. And you had an opportunity to do so before you
5 submitted your reply declaration. Correct?

6 A. I cited to these references, yes.

7 Q. So in this -- in the guidance that you cited
8 in your reply, there are no reversible encryption
9 methods described that would be permitted to get around
10 a derivation requirement. Correct?

11 A. It says, and we've already discussed, that a
12 symmetric cipher can be used in a way that it's not
13 reversible; and it could also -- if you use a public key
14 system, you can set it up so that the keys are not
15 available. So you can comply with this guidance using
16 those functions, which is what it says right there.

17 Q. I'm just reading your testimony off of the
18 real-time. You said that based on -- it said, "that a
19 symmetric cipher can be used in the way that it's not
20 reversible."

21 A. That's correct.

22 Q. Where does it -- where does it disclose a
23 symmetric cipher?

24 A. It doesn't. It says, "associated with such
25 functions are not disclosed." So it's possible to

1 construct cryptographic hash functions not solely from
2 one-way hash functions. And that's what we discussed
3 earlier.

4 Q. Yeah. My question is directed not to what is
5 theoretically possible, but what would be permitted by
6 HHS to be compliant with the HIPAA Privacy Rule.

7 A. Well, it's not what would be permitted; it's
8 what would follow this guidance. And I'm telling you
9 that public key functions or even symmetric ciphers used
10 in the way that we discussed earlier would comply with
11 this guidance.

12 Q. And you've identified no -- is there -- is
13 there any evidence of record that you have available
14 that supports that position?

15 A. Yeah, my CV.

16 Q. So there is no supporting documents that
17 actually disclose the ability to use a symmetric cipher
18 in a manner that's compliant with HIPAA? Correct?

19 A. I don't need to. You -- you are having the
20 opportunity to examine me, Counselor; and I'm telling
21 you that you can comply with this guidance using
22 functions for which the keys are not disclosed, and
23 there are multiple such functions.

24 Q. I'm just trying to be clear that there's no
25 express disclosure in any documents you cited in your

1 declaration that support that position. Correct?

2 A. This document supports it along with my
3 25 years in cryptographic systems, which is why we're
4 having this discussion. The fact that you don't
5 understand that is not my problem, but certainly my
6 expertise comes with my declaration in the form of my
7 CV.

8 Q. I'll just give you one last opportunity.
9 Is there any --

10 A. I already gave you an answer, Counselor. I've
11 had enough of you.

12 Q. Excuse me. Dr. Clark, I'm trying to get a
13 clear answer. This is my time for the deposition.
14 Okay? I'll ask the questions; you can respond.

15 One last time: Can you point to any
16 disclosure of a reversible encryption algorithm that can
17 be used in compliance with HIPAA?

18 A. Asked and answered.

19 Q. Are you refusing to answer?

20 A. I'm not refusing. I've answered it three
21 times. Look at my CV. Look at this guidance, and I'm
22 giving you the answer. You don't like it, but I'm
23 giving it to you.

24 Q. Okay. Let's move on to the Settimi reference,
25 please.

1 Do you have a copy of Settimi available?

2 A. I do.

3 Q. Let's look at paragraph 41, please.

4 A. Yes.

5 Q. This paragraph describes methods for
6 generating an encoded patient identifier, or EPID for
7 short. Correct?

8 A. Yes.

9 Q. That EPID can be generated by a patient care
10 provider, or PCP. Correct?

11 A. Yes.

12 Q. And this paragraph describes how EPID can be
13 generated from, say, a password screen and identifying
14 information for a patient. Correct?

15 A. In this embodiment, yes.

16 Q. That password screen is known only to the PCP.
17 Correct?

18 A. Yes.

19 Q. And the identifying information can be, for
20 example, a patient identifier or other information such
21 as patient name, age, and Social Security number.
22 Correct?

23 A. Correct.

24 Q. And so if the identifying information is not
25 hashed, it would fail to comply with the derivation

1 requirement. Correct?

2 A. No, because the password string that's
3 incorporated, again, would not be shared with anyone
4 else, so the data would not be recoverable.

5 Q. That wasn't my question.

6 I'm asking about the identifying information.
7 Would the HIPAA Privacy Rule require that the -- that
8 the identifying information be hashed --

9 A. Not according to --

10 Q. -- in order to comply with the derivation
11 requirement?

12 A. Not according to the guidance that we've been
13 discussing. And so this password, again, would prevent
14 you from recovering the information unless you have it.

15 So it would meet the guidance because this,
16 again, would be a function, like a cryptographic hash,
17 that would prevent recovery without, in this case, a
18 password.

19 Q. What does the guidance tell us that the
20 derivation requirement -- strike that.

21 As disclosed in paragraph 41, there is a
22 patient identifier encoding software 306. Is that
23 correct?

24 A. That's what it says.

25 Q. And it says that that software hashes the

1 encoded password string to produce a 16-digit number.

2 Correct?

3 A. It does.

4 Q. And there's no disclosure here of hashing of
5 patient identifying information. Correct?

6 A. It's encoding software, and a hash is an
7 encoding. So it doesn't say cryptographic hash; but I
8 understand, reading that, to make it comply with the
9 guidance that we've been discussing.

10 Q. Settimi specifically uses the decrypted EPID
11 to re-identify patients. Correct?

12 A. If they have access to the password, yes.

13 Q. And in order to decrypt the EPID, a one-way
14 function could not be used. Correct?

15 A. A one-way function could not be used and then
16 reversed, that is correct.

17 Q. So a hash would not be used to encode the
18 patient identifying information if the EPID is to be
19 decrypted. Correct?

20 A. No. The -- then the key has to be made
21 unavailable to any recipient of that data. Correct?

22 Q. And in this paragraph, there is a reference to
23 Rivest, Shamir, and Adelman, RSA algorithm. Do you see
24 that?

25 A. That's a public key algorithm such as the one

1 we were discussing previously.

2 Q. Yes. So that public algorithm would be a
3 reversible encryption algorithm. Correct?

4 A. Not without access to the private key.

5 Q. So it is reversible if you have the private
6 key. Correct?

7 A. If you have the private key, you can decrypt,
8 that is correct.

9 Q. So RSA would be -- would not be considered a
10 one-way function. Correct?

11 A. It is not a -- it can be used like a symmetric
12 algorithm, if constructed; but if you want to recover
13 the data, then, no, you can't use a one-way function.

14 Q. And also in paragraph 41, there is a reference
15 to a two-fish algorithm. Correct?

16 A. Two-fish is a symmetric algorithm.

17 Q. And so a symmetric algorithm is also a
18 reversible encryption algorithm?

19 A. If one has access to the key, yes.

20 Q. Are the EPIDs in Settimi stored with
21 the de-identified records in the centralized database?

22 A. I'm sure that they could be, but I would have
23 to search to find out if there's an explicit disclosure
24 of that.

25 Q. Would that have been an important

1 consideration for you in the Evenhaim/Settimi grounds
2 that you proposed?

3 A. Yes, I mean because you have to have a token
4 in order to search the database.

5 Q. So in the Evenhaim/Settimi ground, as you've
6 proposed, the EPID would be stored in the centralized
7 database with the de-identified records; is that
8 correct?

9 MR. OLIVER: Objection. Mischaracterizes.
10 Foundation.

11 THE WITNESS: Right. I mean, that would be
12 one way to implement it, but it -- I mean, basically you
13 have to -- Settimi is -- has a de-identified database,
14 and you would need some means of searching for those
15 records, and EPID would be one way to do that.

16 BY MR. STEPHENS:

17 Q. And if the EPIDs are stored in the centralized
18 database --

19 (Court Reporter requested clarification.)

20 BY MR. STEPHENS:

21 Q. If the EPIDs are stored in the centralized
22 database, is it your contention that the searcher would
23 issue queries that include EPIDs to the centralized
24 database to search for the records of particular
25 patients?

1 A. Maybe, maybe not. Again, it depends on the
2 implementation. That's certainly one way to do it if
3 you wanted to.

4 Q. I'm asking how you described it in your -- in
5 your declarations.

6 A. Again, in my declaration, if it's -- was
7 necessary to be able to search by those tokens, then you
8 would need to include some means of pointing to the data
9 associated with those tokens.

10 Q. Can you just tell me how the -- how does the
11 system operate in the proposed Evenhaim/Settimi
12 combination?

13 A. In the combination, Settimi has a
14 de-identified database that is searchable by the system
15 of Evenhaim.

16 Q. And are you using tokens to search the
17 database in the combination?

18 A. That would be one way to do it, as I said.

19 Q. And what is the, you know -- is it Evenhaim's
20 data aggregator that issues queries to the centralized
21 database?

22 A. It is.

23 Q. Would the -- would the -- strike that.

24 Let's go to your reply declaration again at
25 paragraph 12.

1 A. Okay.

2 Q. At the top of page 10, the last sentence you
3 write that, "Evenhaim's query would be formatted to
4 match the token designed used by Settimi's database so
5 that they speak the same language," correct?

6 A. At paragraph 12? Yes, I see it.

7 Q. Do you have any systems before the Vigilytics
8 patent in which a third party encrypted PII to generate
9 request tokens that could be matched against a
10 de-identified dataset?

11 A. Not from memory.

12 Q. Okay. Let's turn to Evenhaim, please.

13 A. May I close Settimi? I'm having a hard time
14 getting through all this stuff on my desktop.

15 Q. Yeah. Please go ahead and close Settimi.

16 A. Okay. I have it up.

17 Q. And I'll refer to the -- there's a paragraph
18 in Column 4 at lines 34 to 48.

19 A. Okay.

20 Q. And in this paragraph, Evenhaim identifies a
21 significant challenge with measuring the impact of a
22 consumer health program when the health program sponsor
23 does not have the full healthcare information of the
24 target population at their disposal. Correct?

25 A. That's what it says.

1 Q. And then the paragraph refers to
2 de-identification methods under HIPAA.

3 Do you see that?

4 A. Yes.

5 Q. And you're familiar with de-identification
6 methods under HIPAA. Correct?

7 A. Yes.

8 Q. Those could include the safe harbor method and
9 expert determination method. Correct?

10 A. Yes.

11 Q. Under any HIPAA-compliant method for
12 de-identification, PII is removed from the original
13 patient data, at least to the extent that it can't be
14 re-identified; the identity of the patient can be
15 discerned from the record. Correct?

16 MR. OLIVER: Objection. Form.

17 THE WITNESS: Right. So as we've been
18 discussing, that the recipient of such a record, unless
19 authorized that is having access a key, cannot access
20 the PII. And you would be compliant.

21 BY MR. STEPHENS:

22 Q. I'm -- I'll clarify my question.

23 I'm just referring to de-identification
24 methods such as safe harbor or expert determination
25 method.

1 A. And my answer remains the same.

2 Q. Under the safe harbor method -- we'll take
3 that first.

4 To de-identify a record according to the safe
5 harbor method, would you strip PII from the original
6 patient data record?

7 A. I would make it unavailable so if it is one
8 way encrypted or encrypted in a way that it's not
9 recoverable, then I think it would meet that
10 requirement, yes.

11 Q. And the -- under the safe harbor method, the
12 privacy rule defines specific identifiers that must be
13 removed from the protected health information for
14 compliance. Correct?

15 A. Right. They must be unavailable.

16 Q. And, likewise, under the expert determination
17 method -- I guess I'll just ask: How does the expert
18 determination method apply under HIPAA?

19 A. It means that an expert can determine that the
20 privacy of the individuals in the PHI is preserved with
21 a sufficient degree of assurance.

22 Q. So a dataset that was de-identified according
23 to expert determination, would it have less data
24 available than the original dataset, in general?

25 A. Yeah. It would be less data available to an

1 unauthorized user, yes.

2 Q. So under any HIPAA compliant de-identification
3 method, the de-identified dataset will generally have
4 less data available than the original dataset. Correct?

5 A. There -- the PII would be unavailable so that
6 would need to be unavailable. Yes.

7 Q. Now, this paragraph, Evenhaim explains that
8 existing de-identification methods under HIPAA may
9 render the information useless for the purpose of
10 measuring the impact on health programs. Correct?

11 A. That's what it says.

12 Q. Would a POSITA have understood on this
13 disclosure that Evenhaim teaches a way from searching
14 de-identified data under HIPAA?

15 A. No. I don't think so.

16 Q. What does "useless" mean to you?

17 A. Plain English meaning.

18 Q. So how do you, I guess, reconcile -- well,
19 would you acknowledge that Evenhaim criticizes the use
20 of de-identified data under HIPAA?

21 A. No, I don't think so. It says it may render
22 the information useless. So I would understand that to
23 mean that you need to be cautious in how you implement
24 it so that you don't do that.

25 Q. Let's turn to Column 16 at lines 64. And do

1 you see the sentence that says, One cannot query or
2 analyze parameters that are no longer in the lower
3 resolution dataset"?

4 A. Yes. That's what it says.

5 Q. And so that would apply to a de-identified
6 dataset under HIPAA. Correct?

7 A. Not necessarily, no.

8 Q. You just agreed earlier that a de-identified
9 dataset would have less data available than the original
10 dataset. Correct? Data available.

11 A. To unauthorized users, that's correct.

12 Q. And so that data be unavailable to the query
13 to be analyzed. Correct?

14 A. Not if those -- that queries are authorized.
15 So the information is not lost; it's just unavailable
16 which is what they are talking about here. This is --
17 that if you have information lost, then it's lower
18 resolution. And that's the entire point of Evenhaim is
19 how do we de-identify without lowering the resolution of
20 the dataset.

21 Q. Let's -- let's assume that the -- I'm talking
22 about an entity that's -- that does not have -- that's
23 not authorized, does not have access to the data that's
24 rendered unavailable. Okay?

25 In that instance, the information would be

1 lost to that entity, and that entity wouldn't be able to
2 query or analyze the data that it encrypts from the
3 original dataset. Correct?

4 A. It would be unable to use the PII or the PHI
5 insofar as they could link it to an individual. But
6 they were free to use it. All of the other information
7 would be preserved. If they needed the PII, then they
8 would have to be authorized.

9 Q. Anaheim at least expresses a preference
10 against searching de-identified datasets. Correct?

11 A. I don't think so. I mean, that's not the way
12 I read it.

13 Q. Does Evenhaim express a preference for
14 de-identified datasets?

15 A. No, it expresses a preference for datasets
16 that are not low resolution.

17 Q. Is Evenhaim agnostic on the issue of searching
18 de-identified datasets?

19 A. I don't think it's agnostic. The issue is
20 whether or not you have information loss in the system.

21 Q. In the Evenhaim/Settimi combination, the
22 centralized database pulls de-identified records.
23 Correct?

24 A. Yes.

25 Q. And when searching that database, the

1 information that had been stripped as a result of
2 de-identification is unavailable to the search -- to the
3 search. Correct?

4 A. It depends on how you strip it. You can
5 render it unavailable; that is, by encrypting it in the
6 token and render it unavailable without loss of
7 resolution.

8 Q. So let's just take an example. Let's say the
9 de-identified datasets have stripped the zip code of the
10 patients from the data records. Okay?

11 A. Stripped or included it in the token so that
12 it's unavailable?

13 Q. Either way. Okay?

14 A. Yeah, I'm listening.

15 Q. So the searcher would be unable to search
16 by -- search the database by zip code. Correct?

17 A. I mean, again, it depends -- it would depend
18 on who the searcher was and how you were using it, but,
19 yes, generally speaking that zip code would not show up
20 for an unauthorized user.

21 Q. Still in that context, the data would be
22 unavailable to the searcher. Correct?

23 A. To the unauthorized user, yes.

24 Q. And to the unauthorized user, that would
25 appear as a lower resolution dataset. Correct?

1 A. To that searcher, that information would be
2 unavailable, yes.

3 Q. All right. Let's turn to Column 5, please,
4 and at line 46 there's a paragraph that describes health
5 program.

6 Do you see that?

7 A. I do.

8 Q. And Evenhaim explains here that, "Typically
9 patients, consumers, or healthcare professionals will
10 opt in to participate in such a program," correct?

11 A. That's what it says.

12 Q. What does it mean to opt in to a health
13 program?

14 A. That means to agree to participate.

15 Q. So if patient is agreeing to participate in
16 the health program, they would be authorizing the use of
17 their medical information for that program. Correct?

18 A. I would expect so.

19 MR. STEPHENS: Okay. I don't think I have
20 much more, but can we take five minutes, and I'll review
21 my notes, and we'll see if we have anything further.

22 THE WITNESS: Okay.

23 MR. STEPHENS: Thanks.

24 (Recess: 1:16 p.m. 1:21 p.m., EST.)
25

1 BY MR. STEPHENS:

2 Q. Dr. Clark, at any point during our breaks
3 today, did you discuss the substance of your testimony
4 with Counsel?

5 A. I haven't spoken to Counsel at all.

6 Q. Anyone else?

7 A. Nope.

8 MR. STEPHENS: All right. No further
9 questions.

10 MR. OLIVER: Thank you. I have no questions
11 for the witness.

12 MR. STEPHENS: All right. Thank you for your
13 time, Dr. Clark.

14 THE WITNESS: All right. Thank you.

15 COURT REPORTER: Counsel, may I get transcript
16 requests on the record? Mr. Oliver?

17 MR. OLIVER: Yeah, I don't need a transcript.
18 It's going to be submitted in the record so -- and will
19 be done probably next week, so I don't need a copy.

20 (Whereupon the proceedings concluded at
21 1:22 p.m.)

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 v. VIGILYTICS

DATE OF DEPOSITION: MARCH 20, 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 _____

Page _____ Line _____ Reason _____

From _____ to _____

Deponent's Signature _____

Date _____

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

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 March 20, 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

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

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

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

Dated: 24th of March, 2025.

TAMARA L. HOUSTON
CSR 7244, RPR, CCRR 140

THE SULLIVAN GROUP OF COURT REPORTERS

- --o0o-- 6:2,5,9 0 012 7:23 1 1 18:15 34:10,12 40:23 41:2 52:19 54:15 55:18, 25 56:1 10 70:2 1001 17:20 1003 8:15 1004 9:9 1008 52:11 1009 9:9 1015 8:13,20 1016 26:4,8,11 27:2 57:12, 15,19 10:09 6:1 118 22:21 23:8 28:4 47:4 11:09 34:7 11:20 34:6 11:24 34:7 12 40:24 69:25 70:6 12:01	50:9 12:06 50:8 12:10 50:9 12:24 55:16 12:28 55:16 13 45:17 130 23:2 47:2,5 48:10 14 42:11 56:1 140 47:3,11,20 48:1,8 142 47:2 15 10:10 150 18:5,11,17 21:20 22:2 154 22:22 28:4,10 16 73:25 16-digit 66:1 164.514 25:2 164.514(c) 58:4 17 47:1 19 52:15 57:5 1:16 77:24 1:21 77:24 1:22 78:21	2 2 18:1,4,14 21:21 53:25 20 6:1 40:14 200 23:1 2006 24:24 53:21 2024-00307 8:20 2025 6:1 203 18:17,21 20:1 204 20:20 205 18:9,18 20:2,4 206 18:10 20:21,25 21:8,15 208 21:15,23 22:5 23:7 210 18:10 21:5,14,24 22:19 28:1,14 29:5 212 21:20 22:2,5 22 13:6 25 63:3 28 35:7 3 3 40:13 44:24 30 51:7 57:12 302 40:18 42:15 45:1	304 46:11 306 35:10,16 40:18 42:15 45:2,5,11,18,24 46:7, 10,13,17 65:22 31 57:13,21 312 45:3 46:22 328 36:20 34 13:15 22:13,17 27:21 32:1,2 40:25 45:10 50:12,16 70:18 35 32:12 40:25 37 22:17 45:10 375 7:23 39 32:14 4 4 46:24 70:18 404 35:13 36:16 40:19 42:13,14 45:18,19 405 35:15,18 36:16,19 41 32:14 64:3 65:21 67:14 42 27:21 32:2 46 32:12 77:4 48 70:18 5 5 22:13 26:13 27:21 32:2,
--	--	---	---

THE SULLIVAN GROUP OF COURT REPORTERS

19 40:16 52:14 77:3	54:7	agree 16:23 45:5 47:18,25 77:14	appears 41:25
500 43:10	ability 62:17	agreed 12:5 74:8	applied 48:16
56 53:8	absent 48:1	agreeing 77:15	applies 60:4
	accept 12:19 57:17	agreement 30:12	apply 39:8 58:17 72:18 74:5
6 35:4,6 45:16 53:7	access 12:18 22:20 23:6,12,15, 20,24 28:3 30:4 36:18, 23 53:18 55:1 60:15 66:12 67:4,19 71:19 74:23	ahead 70:15	argue 55:2
64 73:25	accompanied 8:5	aimed 16:17	art 11:8,12,18 33:3 35:2 60:25
65 53:8	account 42:6	algorithm 57:4 63:16 66:23,25 67:2,3,12,15,16,17,18	asserts 12:6
651 7:23 8:19,23 11:23 12:16 13:9,16,19 14:5 17:19,20 18:2,24 19:14 20:16 27:17 29:17 32:2, 8,23 33:2,5 34:9,23 35:2 37:18,20 50:12 57:6	Accountability 13:24	allergies 19:11	assigned 54:4
685 7:23	accuracy 14:2	allowed 23:24	assume 7:13 15:5 22:7 46:4 74:21
	acknowledge 73:19	allowing 53:16 56:7	assurance 72:21
7 11:25 45:10 52:14	acknowledges 51:9	ambiguity 59:21	attached 48:13
700 43:11	acquiring 52:1	amount 10:3	attacker 42:8
7244 6:4	Act 13:24	Anaheim 75:9	attainable 46:16 47:19,23
	additional 41:20	analyses 34:24	attempts 42:5
8 32:9	address 53:2	analysis 37:16,24 38:2,7,14,16 39:7,13,17,19,25 40:2 42:25 60:19	auditing 43:3
	addresses 27:6	analyze 74:2 75:2	authority 60:7
9 40:12 42:10	Adelman 66:23	analyzed 74:13	authorized 71:19 74:14,23 75:8
	age 64:21	and/or 35:19 51:6 53:2 56:8	authorizing 77:16
A	aggregator 18:10 20:6,8,21,25 21:8,15 69:20	anticipated 23:23	aware 10:13 14:16,21 15:2 60:7
a.m. 6:1 34:7 50:9 55:16	agnostic 75:17,19	appearance 6:20	
abide			B
			back 18:11 21:20 27:17 34:6

THE SULLIVAN GROUP OF COURT REPORTERS

42:10 50:8 51:7 55:18 57:5	business 23:12,24 30:6	charged 16:24	60:16 62:24 63:13
background 13:16	button 12:25	chat 12:15 13:3 17:24 24:24 26:4	clearing 21:11
based 18:23 22:8 32:1 37:2 39:25 42:20 59:20 61:18	C	check 44:15	cleverly 18:15
basically 68:12	caching 48:9,14 56:19,21	checked 10:11	close 26:5 70:13,15
batch 32:16,20,21,23,25 33:2, 6,10,12,13,16,20,24	California 6:4	checks 42:12	closed 53:23
begins 12:4 26:16 32:11 35:6 40:13 57:24	called 6:7 41:6	cipher 48:23,24 49:10,16,17, 21,22 50:3 52:20 56:17 61:12,19,23 62:17	code 45:20 54:5 58:18 76:9, 16,19
behalf 6:17,22	capable 54:17	ciphers 48:20 62:9	column 22:13 27:21 32:2,9 35:4 40:12,24 42:10 45:10, 16 46:24 52:14 53:7 55:18,25 56:1 70:18 73:25 77:3
beneath 55:19	care 64:9	circumstances 60:12	combination 69:12,13,17 75:21
benefits 51:9	case 15:9 33:5 49:1 51:2 65:17	cite 57:12	combined 55:3
beta 18:8	cases 6:14	cited 26:8 40:23 57:21 60:18, 21 61:6,7 62:25	communication 9:12
birth 45:20	cautious 73:23	civil 15:1,6,19,21	compare 43:4,6
bit 39:9	centralized 67:21 68:6,17,21,23 69:20 75:22	Claim 34:10,12 40:23 41:2	compared 44:19
bits 59:2	Certified 6:4	claimed 11:9	comparison 42:25
breaching 31:23	challenge 70:21	claims 21:11	complete 56:21 59:20
break 7:16,18 34:3	change 22:11	clarification 68:19	completely 7:3
breaks 78:2	channel 45:8	clarify 71:22	compliance 14:6,10,13 16:8 50:19, 22,25 51:15,20 54:8 63:17 72:14
bring 24:22	channels 9:12	clarity 39:5	compliant 30:11 31:12 51:22 55:6 60:8 62:6,18 71:20 73:2
broader 25:17	characteristics 13:22 34:16	Clark 6:6,11,24 9:1 28:21 34:9 39:3 60:16 63:12 78:2,13	complied 15:17
building 52:4	characterization 26:21 27:13	class 49:15	comply 12:8 13:23 15:11 16:16 17:12 52:2 54:23 60:12
built 51:4	characterizes 34:14	clear	
	characterizing 13:20		

THE SULLIVAN GROUP OF COURT REPORTERS

61:15 62:10,21 64:25 65:10 66:8	contemplates 51:10,17	16:12,16,17 17:14	75:2 76:10,21
complying 16:18	contention 68:22	Couple 10:23	database 14:13 51:24 67:21 68:4, 7,13,18,22,24 69:14,17, 21 70:4 75:22,25 76:16
composed 34:14	context 32:23 76:21	court 6:3 68:19 78:15	databases 12:8
comprising 34:13	continuing 40:19	covered 23:11,23 26:3 30:6,8,9, 13 31:20 54:6	dataset 70:10 72:22,24 73:3,4 74:3,6,9,10,20 75:3 76:25
computationally 48:12	copies 9:5	create 33:8 36:16 48:21 49:8 58:18	datasets 75:10,14,15,18 76:9
computer- implemented 13:19 34:12	copy 12:16 17:21 52:7 53:22 64:1 78:19	creating 20:16 33:13	Datavant 6:22
concept 28:20 37:6 41:6	correct 8:1,6 9:6 11:9 14:3,6, 10,18 17:17 18:18 20:2, 21 21:16,20,24 22:2,23 23:3,16 24:12,15,16 25:7,11 26:9 27:15 28:5,10 29:7,11 31:16, 24 32:3,17,24 33:9,14, 17,22,25 34:24 35:10, 13,16,20 36:11,16,20 40:8,9,21,24 41:5,25 42:23 43:2,13,23 44:1, 8,16 45:3,12,21 46:1,8, 9,11,14,17,22 47:11 48:1,6,10,11 49:2,24 50:20 51:12 52:18,23 53:2,5,13,17 54:8,11, 21,24 56:11,14,20 57:2, 10,13,16,22 58:9,18 60:3,20 61:5,10,21 62:18 63:1 64:7,10,14, 17,22,23 65:1,23 66:2, 5,11,14,16,19,21 67:3, 6,8,10,15 68:8 70:5,24 71:6,9,15 72:14 73:4,10 74:6,10,11,13 75:3,10, 23 76:3,16,22,25 77:10, 17	criminal 15:2,6,19,21	date 35:22,24 36:2,3,9,15, 19,23 37:10,15,21 38:3 45:20
concerned 14:5,9,13 15:18 29:17 51:14		criticizes 73:19	dates 35:20
concluded 78:20		cryptographic 48:11,14 49:7,10,18 58:6 59:2,6,25 62:1 63:3 65:16 66:7	de-identification 13:22 15:15 17:6,14 20:17 29:2 51:10,18 57:10 71:2,5,12,23 73:2,8 76:2
condition 19:10 30:18 31:2		cryptography 49:15	de-identified 20:11,13 21:15,23 22:5, 18 23:7,16,21 26:24 27:8,25 28:7,9,15 29:3, 6,10,19 30:5,9,15 31:9, 12,15 33:19 34:15 47:3, 11,19,25 48:6,8,17 49:12 53:11,16 54:5 56:10 58:9 59:9 67:21 68:7,13 69:14 70:10 72:22 73:3,14,20 74:5,8 75:10,14,18,22 76:9
conditions 31:19		current 19:11 43:5	de-identifier 47:2
confirm 9:14		CV 9:10 62:15 63:7,21	de-identify 16:11 51:6 72:4 74:19
confirms 45:10		D	de-identifying 27:8 56:6
consideration 51:1 68:1		data 13:21 15:14 18:9,10,17, 20,24 19:2,14,17,22 20:1,5,6,7,8,11,13,15, 21,25 21:2,4,7,14,15, 19,23 22:1,5,6,18,19 23:5,7,11,15,16,20,21, 23 27:24,25 28:1,2,7,8, 9,13 29:3,5,6,10,18,19 30:4,15 31:9,12 33:19, 22 34:16 35:13,15,18 36:16,19,24 40:19 42:2, 13,14 43:18 45:18,19 47:3,11,20 48:1,5,8 51:18 52:3,5 53:11,13 56:6,8,10 60:15 65:4 66:21 67:13 69:8,20 71:13 72:6,23,25 73:4, 14,20 74:9,10,12,23	dealing 41:11
considered 11:3 67:9	correctly 34:18		dec 9:23 57:22
constitute 26:20	counsel 6:19 9:12 10:1,18 78:4, 5,15		
construct 49:16 62:1	Counselor 38:20 49:14 62:20 63:10		
constructed 67:12	countermeasures		
constructing 49:21			
consumer 70:22			
consumers 77:9			

THE SULLIVAN GROUP OF COURT REPORTERS

declaration 8:3,4,14,19,22,23 9:20 11:22 12:6,13,16 13:16 50:11 51:8 57:6 60:19 61:5 63:1,6 69:6,24 declarations 7:22,25 8:8,10,12,17 9:8,24 10:6,14 11:4,7 26:9 38:23 40:4 69:5 decrypt 46:20 48:25 49:19 50:3 57:1 66:13 67:7 decrypted 46:17,21 49:23 66:10, 19 decrypting 49:2 decryption 49:4 50:2 decrypts 33:20,24 default/deny 37:8 define 17:5 defined 12:12 24:18 32:22 40:20 41:4,15 42:22 defines 72:12 definition 12:5 13:8,11 definitions 38:25 degree 72:21 depend 76:17 depending 22:11 30:18 42:2 46:2 depends 23:17 29:12 43:14 49:5 69:1 76:4,17 deposition 6:25 9:18 10:17,22 55:5 63:13	derivation 54:11,14,24 55:3,6 58:12,15 59:5 61:10 64:25 65:10,20 derived 53:4 54:16,20 55:10 58:5 describes 19:14 20:16 33:10 34:23 51:17 52:17 53:10 55:21 56:4,19 64:5,12 77:4 describing 52:19 design 17:1 50:17 designed 70:4 designing 17:10 desire 51:21 desktop 70:14 detail 39:10 details 35:19 determination 58:7 60:1 71:9,24 72:16,18,23 determine 72:19 device 34:13 45:1 diagnoses 40:11 diagnosis 35:20 36:6,9,15 37:11 Dick 51:9,10,14 Dick's 51:19,22 52:1 difference 21:22 22:4,9 24:8	directed 62:4 directory 9:7 disagree 26:21 27:12 disallows 41:3,14 discerned 71:15 discharge 36:2 disclose 17:7 59:13 61:22 62:17 disclosed 16:13 58:8 59:8 60:3,5 61:25 62:22 65:21 disclosure 15:15 25:19 27:20 32:1 47:16 62:25 63:16 66:4 67:23 73:13 disclosures 16:2 25:3,11 discuss 78:3 discussed 9:4,21 10:2 22:2 41:7 45:22 51:5 53:3 57:3 61:11 62:2,10 discussing 47:8 49:6 56:15 65:13 66:9 67:1 71:18 discussion 63:4 disposal 70:24 distinction 25:15 docs 12:25 doctor 37:17,22 38:5,6,12,13 document 63:2 documents	62:16,25 doubt 14:19 draft 9:25 drafted 10:1 drafting 10:4 E e.g. 22:19 28:1 e.g. 40:20 earlier 8:14 29:23 42:21 43:9, 12 44:6 45:23 49:11 51:5 53:3,20 54:19 57:3,15 62:3,10 74:8 easier 13:3 easily 55:11 Eastern 34:6 50:8 electronic 9:1,5 email 9:15 emails 9:16 embodiment 20:10,22 21:17 22:3 23:10,22 28:11 32:8,18 33:18,23 36:17 46:12, 15 52:20 53:6,14,18 55:2,9 56:15 64:15 employ 17:13 empowered 56:8 encode 66:17 encoded
---	--	--	---

THE SULLIVAN GROUP OF COURT REPORTERS

64:6 66:1	EST 34:7 50:9 55:16 77:24	explains 22:17 23:1 32:15 36:18 45:17 58:16 73:7 77:8	figure 18:1,4,13,14,15 20:10 21:6,10,21 32:19 44:24 45:1 52:19
encoding 65:22 66:6,7	Evenhaim 69:15 70:12,20 73:7,13, 19 74:18 75:13,17 77:8	explanation 14:3 59:24	file 12:15 32:16,20,21,22, 24,25 33:2,7,10,12,14, 16,20,24 52:3
encompass 16:8	Evenhaim's 69:19 70:3	explicit 67:23	files 9:6
encounter 38:4 39:15	Evenhaim/settimi 68:1,5 69:11 75:21	explicitly 50:17 51:16 57:9	finally 21:19
encounters 41:7	evidence 27:10 62:13	express 62:25 75:13	find 67:23
encrypt 45:7,8 48:25 49:19 57:9	EXAMINATION 6:10	expresses 75:9,15	fine 15:8 34:4 50:7
encrypted 32:16 33:12,16 45:6,11, 24 46:1,5,16 48:21 49:8 52:17,21,22 53:4,15 54:19,23 55:5 56:20 57:1 70:8 72:8	examine 62:20	extent 71:13	fix 55:11
encrypting 33:6,10 76:5	examples 19:24 25:25 26:19 45:22 53:1	F	fixed 10:15
encryption 45:2 46:8,22 48:15 49:3 56:6,14 58:23 61:8 63:16 67:3,18	exceptions 58:14 59:5	face 15:20,21	flawed 27:1,3,15
encrypts 33:8 75:2	excuse 27:25 49:25 63:12	facility 34:17,21 38:4	flow 18:8
English 34:22 35:3,24 36:8 37:20 38:18,21,25 39:8, 10,17 73:17	executed 32:22 33:3	fact 33:5 46:21 63:4	focus 8:16
ensure 56:6	exhibit 8:13,15,20 17:20 24:24 26:4,8,11 27:2 52:11 53:21 57:12,15,19 60:18	fail 64:25	follow 12:22 39:5 62:8
entire 74:18	exhibits 9:8	failed 42:4	form 17:2 23:9 28:16 29:20 45:13 46:1 56:25 59:11 63:6 71:16
entities 56:9 61:2	existing 73:8	fails 15:11	formatted 70:3
entity 23:12,24 30:6,9,13 31:16,20 53:11,17 54:6 74:22 75:1	expect 51:20 77:18	fair 7:14 18:8	formatting 22:10
EPID 64:6,9,12 66:10,13,18 68:6,15	expert 39:20,21,23,25 40:7,9 49:25 58:6 60:1 71:9,24 72:16,17,19,23	fall 7:7	forming 56:20
EPIDS 67:20 68:17,21,23	expertise 63:6	familiar 15:4 17:4 19:2 24:7 28:20 71:5	Foundation 23:9 47:12 55:7 68:10
errors 10:13	explain 20:12 23:19 25:15 37:1 39:23 41:8	features 23:1 40:23 51:21 52:1,6	fourth 6:13 12:3 51:8
	explained 23:22	feed 9:11	free 22:15 75:6
		feel 22:15	frequency
		field 50:1 55:20 56:1	

THE SULLIVAN GROUP OF COURT REPORTERS

41:12,21 full 70:23 function 20:23 49:18 58:17 59:7, 8 65:16 66:14,15 67:10, 13 functions 48:15,16 57:9 58:6,8 59:3 60:1,3 61:16,25 62:1,2,9,22,23 fundamental 26:17	government 61:2 governs 14:14 25:10 granularity 41:11,12 Great 11:15 ground 68:5 grounds 68:1 group 13:20 19:18,19 22:21 23:8 28:4,10 29:7,15 30:16 32:21 34:14 35:13 45:19 46:14 guess 18:23 25:23 37:17,21 72:17 73:18 guessing 22:10 42:7 guidance 26:12 27:1,2 57:16,25 58:13,16,20,22,24,25 59:18,25 60:6,11,17,22, 23 61:3,7,15 62:8,11,21 63:21 65:12,15,19 66:9 guys 13:14	57:9 58:6,17 59:2,6,7, 25 62:1,2 65:16 66:6,7, 17 hashed 56:25 57:3 64:25 65:8 hashes 48:16 49:7 65:25 hashing 66:4 heading 25:8 health 13:23 15:10 17:11 19:10 23:2 24:14,17 25:4,11,15 26:17,25 27:5,8 30:17 31:1,3,19 36:10 48:9 70:22 72:13 73:10 77:4,12,16 healthcare 14:14 19:1,18 33:22 34:17,21 36:1,3 38:4 39:22 40:7 53:10,16,17 70:23 77:9 healthcentric 24:9 hear 19:6,13 HHS 26:12 57:16 58:14 61:2 62:6 HIPAA 12:9 13:24 14:5,9,13, 17,23 15:3,5,11,13,22 16:16,18,20 17:4,12,16 24:18 25:7,10,13,19 26:5,12 30:8,13 36:11 37:9 50:18,22,23,25 51:9,14,17,19,22 52:2,6 54:8 57:9 58:12 60:9 62:6,18 63:17 65:7 71:2,6 72:18 73:2,8,14, 20 74:6 HIPAA-COMPLIANT 71:11 Hold 55:23 home 24:4	hospital 18:5,11,17 21:20 22:2 hour 7:17 30:7 34:3 hours 10:7,8,23 housekeeping 6:14 houses 21:11 Houston 6:3 hundreds 43:21
G gave 63:10 gender 45:20 general 32:6 72:24 generally 12:4 51:10 55:1 73:3 76:19 generate 22:10 47:3 70:8 generated 64:9,13 generating 64:6 generator 36:20,24 46:8 give 19:24 48:19 63:8 giving 59:20 63:22,23 goal 50:18 51:19 goals 51:19 Good 6:11 govern 25:19	H half 30:7 hand 16:20 handled 17:10 handles 15:10 harbor 71:8,24 72:2,5,11 hard 70:13 hash 48:12 49:18 56:22,24	I ID 52:21 53:4,15 54:20,23 55:5 56:20 57:1 idea 28:24 39:14 identifiable 16:13 22:21 23:7 24:10 28:3 47:4 identified 11:3 19:21 25:16 29:4 35:18 42:20,21 43:1,7, 10,11,12,25 44:14 62:12 identifier 64:6,20 65:22 identifiers 45:21 72:12 identifies 70:20 identify 26:2,22 27:6 28:24 54:18 58:20,22 identifying 24:11 35:12 40:19 42:13,14 43:18 44:13 45:18,19,25 52:22,25 64:13,19,24 65:6,8 66:5,18 identities 29:14 44:15,19	

THE SULLIVAN GROUP OF COURT REPORTERS

identity 41:23 47:9,18 71:14 IDS 52:17 impact 70:21 73:10 implement 15:10,16,24 16:20 22:12 30:21 31:21 36:22 43:22 51:21 56:5 60:25 61:3 68:12 73:23 implementation 14:20 54:1 69:2 implementations 58:12 implemented 15:12 16:3 23:18 29:13 39:18,20,21 40:7,9 43:15 46:2 implementing 14:12,15,22 15:22 16:25 48:2 52:6 61:1 imply 39:15 important 23:5 50:25 67:25 impose 15:6 imposed 14:17 include 9:9 16:7 19:17 31:11 35:12 45:19 50:22 53:1 68:23 69:8 71:8 included 18:20,24 19:3 21:3 41:4,15 46:6 76:11 including 58:8 59:9 incomplete 27:14,16 incorporated 65:3 increase 28:13 41:24	incurred 14:22 independently 10:24 index 38:3 indicator 18:5 individual 19:21 28:24 32:15 33:1 41:24,25 47:9,18 53:5 54:17,21 75:5 individual's 41:17 individually 13:2 individuals 13:21,22 19:18,19 23:8 28:10,13 29:6,14,15 30:15 31:10 34:15 35:13 41:3,15 43:1,6, 10,11,25 44:6,7,14,15, 20 46:14 51:24 72:20 individuals' 34:16 infeasible 48:12 infer 31:2 42:9 inference 41:13,20,22 42:24 inferring 41:23 information 13:20 15:11 16:13 17:11 19:19 22:21 23:2, 8 24:11,15,18 25:4,11, 16 26:17 27:5 28:3,18 31:3 34:14 35:20 36:6, 9,11,15 37:7,11 38:1 41:13,20 45:25 46:3,4 47:4 48:9,13,17,22,25 49:8,12,13 52:22,25 53:5,16 54:6,16,18,20 55:9 58:9 59:10 64:14, 19,20,24 65:6,8,14 66:5,18 70:23 72:13 73:9,22 74:15,17,25 75:6,20 76:1 77:1,17	informative 39:1 instance 74:25 Insurance 13:23 intended 23:11 33:3 interested 44:3 51:23,25 52:5 interpretation 39:8 Interruption 24:3 invention 55:20,21 56:2 inventions 11:9 invoke 44:22 invoked 42:19 43:13,21 44:5 involve 42:25 involves 43:21 IPR 8:19,20 12:16 50:12 IPRS 7:23 irreversible 47:19 irreversibly 47:3,10,25 48:6,8,17,21 49:8,11 issue 14:9 21:9,10 68:23 75:17,19 issues 9:22 50:18 69:20 items 6:15	J Joe 30:20 Justin 6:21 K key 46:19 48:24 49:4,20 50:2 52:20 53:12,19 55:1 56:5,16 59:1,12, 13,15,23 60:4,5,8,13,14 61:13 62:9 66:20,25 67:4,6,7,19 71:19 keys 58:7 59:8 60:2 61:14 62:22 knew 15:20 29:14 knowingly 14:22 15:3,22 knowledge 12:7 40:1 knowledge-based 40:1 L Landi 50:17 52:7,17 55:18 56:13,19,24 59:13 Landi's 53:4 54:19,23 55:5 language 70:5 large-scale 41:19 law 14:17 15:4 60:8 lawyer 14:24 legally 56:8 level 16:10
--	--	---	--

THE SULLIVAN GROUP OF COURT REPORTERS

liability 15:1,2,19,21 16:2 light 38:22 likelihood 28:13 likewise 36:5 51:25 55:4 72:16 limit 41:21 limitation 41:2 limited 9:7 limits 41:13 lines 27:21 32:2,14 40:24 45:10,16 52:14 53:8 59:25 70:18 73:25 link 75:5 list 11:3 listening 76:14 literally 43:19 logins 42:6 long 60:13 longer 7:18 74:2 looked 53:20 57:15 loops 18:8 loss 75:20 76:6 lost 74:15,17 75:1 low 75:16	lower 74:2,17 76:25 lowering 74:19 lunch 7:18 M made 66:20 maintain 23:1 make 6:20 16:12 37:7 47:15 58:16 59:21 60:14 66:8 72:7 manner 12:8 62:18 March 6:1 marked 8:13,14 match 42:14 43:17 70:4 matched 70:9 matches 44:3 matching 33:21 materials 9:2 10:24 11:2,3 meaning 24:18 34:22 35:3 36:8 37:20 38:18,21 39:10, 17 73:17 means 37:6 39:24 53:15 68:14 69:8 72:19 77:14 measure 38:3 measures 36:22 measuring 70:21 73:10	mechanisms 49:7 medical 12:7 14:12 34:15 36:10 40:10 77:17 meet 65:15 72:9 meeting 10:25 member 45:19 memorized 36:25 37:12 memory 12:14 19:16 24:21 25:14 37:13 51:16 70:11 message 35:9,12,16 40:18 45:2, 5,11,17,24 46:7,10,13, 17 messaging 9:16 messed 55:24 method 34:13 58:7 60:1,8 71:8, 9,11,25 72:2,5,11,17,18 73:3 methods 51:10 56:5 58:23 59:1, 24 60:4 61:9 64:5 71:2, 6,24 73:8 minimum 6:15 minute 55:14 minutes 50:5 77:20 Mischaracterizes 31:17 47:13 68:9 mode 56:18 model 37:8	moment 15:5 22:14 25:24 32:12 52:15 months 40:20 morning 6:11,12 motivated 15:9,16 17:12,13 move 63:24 moved 9:7 multiple 34:15 60:24 62:23 N names 27:6 30:15,22 31:9,11, 15,18 32:7 necessarily 15:18 23:17 42:1 74:7 needed 56:10 75:7 negligent 14:25 network 32:17 33:11,17 45:9 Nick 6:16 NIST 57:25 58:14,25 61:2 nonetheless 15:23 nonidentified 35:15 36:16,19,23 note 43:22 notes 77:21 number 6:4 9:5 19:4,7,24 22:11 26:23 41:21 42:4 43:25 44:6,7,13 53:2 64:21 66:1
---	---	---	--

THE SULLIVAN GROUP OF COURT REPORTERS

numbers 27:7 O oath 6:25 Object 59:11 Objection 17:2 23:9 28:16 29:20 31:17 44:9 45:13 47:12, 21 55:7 68:9 71:16 objective 47:14 obvious 59:4 occur 10:19 30:16 occurs 39:16 48:5 offered 11:7 39:7 Oliver 6:21 17:2 23:9 28:16 29:20 31:17 34:5 44:9 45:13 47:12,21 55:7 59:11 68:9 71:16 78:10, 16,17 one-way 48:16 49:16,21,22 50:3 62:2 66:13,15 67:10,13 open 9:3,12,15 11:22 12:21 13:5 operate 69:11 operating 12:8 operations 32:21 33:4 opinion 31:25 opinions 9:21 11:6 opportunity 61:4 62:20 63:8	opposed 9:25 opt 77:10,12 order 13:23 41:13,22 44:22 55:1 65:10 66:13 68:4 ordinary 11:8,12 original 71:12 72:5,24 73:4 74:9 75:3 outlined 15:14 output 49:3,22 50:3 overlap 24:16 25:18 owner 6:17 owners 56:7 P p.m. 50:9 55:16 77:24 78:21 pages 57:12 paragraph 11:25 13:6,15 22:15,25 26:15,16 32:11 35:6,9 36:14 40:13 42:10 50:12,16 51:7 55:19 56:4 57:5,8,24 58:3 64:3,5,12 65:21 66:22 67:14 69:25 70:6,17,20 71:1 73:7 77:4 parameters 74:2 part 33:6 participate 77:10,14,15 party 18:9,18 20:2,4 22:20 28:2 70:8	passage 52:17 password 42:4,7 64:13,16 65:2, 13,18 66:1,12 patent 6:17 8:19 11:23 13:9, 16,19 14:5 17:19,21 18:2,24 19:14,23 20:16, 18 22:17 23:19 27:17 29:17 30:3,4 32:2,14,23 33:8 34:10,23 35:2 36:18,22 37:1,3,18,20 45:17 70:8 patents 7:23 8:2 14:9 path 15:23 patience 39:4 patient 26:2 39:14 49:2 52:22, 25 53:1,11,13 56:6,7,8 64:6,9,14,20,21 65:22 66:5,18 71:13,14 72:6 77:15 patient's 26:22 30:22 31:24 patients 27:7 28:14 42:13,19 43:17 56:9 66:11 68:25 76:10 77:9 PAUL 6:6 PCP 64:10,16 penalties 14:16,21 15:6 perform 20:7 40:2 49:18 performed 39:19 performing 34:24 period 15:25 16:5 40:20 41:4, 12,16 42:5,6,22	permitted 61:9 62:5,7 person 11:8,12,18 16:10 37:5 47:6 60:11 personally 16:12 22:21 23:7 24:10, 11 25:16 28:3 45:25 47:4 perspective 11:7,17 37:9 petition 8:6 Petitioner 6:19,22 Petitioner's 60:17 pharmacies 21:12 PHI 24:8,14 25:17,20,22,25 26:3,20 32:6 47:2,5,16 51:6 58:5 72:20 75:4 phone 26:23 27:6 phonebook 26:24 phrase 7:6 PII 15:15 17:7,15 20:14 23:12,16,21,25 24:8,11 25:20,22,25 26:20 28:12 29:19 30:5,10 32:6 33:8 36:16 37:11 46:14,16 48:1,3 51:6 56:19,25 57:10 58:17 70:8 71:12,20 72:5 73:5 75:4,7 PIIS 45:22 53:3 place 30:12 plain 34:22 35:3,24 36:8 37:20 38:18,21,25 39:8, 10,17 73:17
--	---	---	--

THE SULLIVAN GROUP OF COURT REPORTERS

plan 7:17 pod 24:4 point 59:20 63:15 74:18 78:2 pointing 69:8 population 70:24 Portability 13:24 POSA 11:11 12:5,6,12 13:9,12 14:12,16 15:9,12,20,24 16:23 17:3,10 37:10 pose 42:1 POSITA 11:11 35:22 36:5,6 37:3 39:6 51:1,20,21,25 55:10 73:12 position 62:14 63:1 possessed 30:14 possibility 29:9 post-encounter 34:17,20,24 35:1,19 37:16,24 38:2,7,14,15 39:7,13,19 pre- 34:17,20,24 35:1 37:15, 24 38:2,7,13,15 39:7, 13,19 pre-encounter 35:19 preclude 24:2 58:4 preference 75:9,13,15 preferred 56:18 prepare 9:20 10:16	preparing 10:6,22 present 55:21 presents 50:17 preserve 41:16 preserved 72:20 75:7 prevent 41:13,19,22 42:3,7 65:13,17 preventing 42:23 previous 19:10 41:7 42:14 43:3, 4,18,20 44:17,22 previously 42:21 67:1 printed 9:2 prior 12:5,13 privacy 14:17 15:7 23:2 25:7, 10,13 31:24 41:17 43:12 50:23 51:24 52:5 53:20 56:7 62:6 65:7 72:12,20 privacy-preserving 41:3 42:18 private 13:21 53:12,19 59:13, 23 60:5,14 67:4,5,7 privilege 37:6 probability 41:23 problem 42:24 55:12 63:5 proceed 15:23 proceeding 12:17 17:20	proceedings 8:1,5,10,14 9:22 10:6 52:11 78:20 process 47:2 processes 51:11 processing 20:7 processor 18:10 21:2,5,14,19,23 22:1,6,19 23:6,11,20,23 27:25 28:1,2,8,14 29:5, 18 30:4 33:3 processors 23:15 produce 48:17 66:1 produced 33:13 48:9 producing 13:20 professionals 77:9 program 70:22 77:5,10,13,16,17 programs 73:10 proper 57:4 properly 47:22 48:7 57:4 proposed 68:2,6 69:11 protected 15:10 17:11 23:2 24:14, 17 25:4,11,15 31:3 36:10 48:9 72:13 protecting 51:24 protection 17:15 provide 19:8 31:8,15 37:10 39:9 49:11	provided 16:25 17:14 22:18 28:1, 8 42:12 49:11 58:7 60:2 provider 64:10 providers 14:15 provision 24:1 54:14 58:3 provisions 54:7 prudent 31:4 pseudonyms 30:19 PTAB 9:22 39:1 public 52:20 56:16 59:1,12,14, 23 60:4,8,13 61:13 62:9 66:25 67:2 pull 52:9 pulls 75:22 purpose 48:13 73:9 purposes 53:12 put 12:16 13:2 17:24 24:23 26:4 Q queries 42:9 46:13 68:23 69:20 74:14 query 21:10 70:3 74:1,12 75:2 question 7:8,9,13,14 19:6 24:5,6 30:7 38:9,10,11 62:4 65:5 71:22 questions 6:17 7:3,6 8:17 11:17 63:14 78:9,10
--	---	--	---

THE SULLIVAN GROUP OF COURT REPORTERS

quickly 17:24	recess 34:7 50:9 55:16 77:24	23,24 71:23	removed 20:14 71:12 72:13
quote 23:6 32:15	recipient 59:14 66:21 71:18	refers 24:14 34:12 35:9 41:2 71:1	removing 47:3
R	recipients 58:9 59:9	refresh 25:14	render 73:9,21 76:5,6
re-ask 24:5	recognizes 32:3	refusing 63:19,20	rendered 74:24
re-identification 23:14 28:21,23 29:10, 18,24 30:1,16 31:5 54:2,5 56:13 58:3,18	recollection 56:21	regard 9:21 15:14,15	reopen 53:23
re-identified 53:17 54:6 71:14	recommend 31:7,8,11	regulations 16:20	repeat 7:9,12
re-identify 28:14 30:21 53:19 56:9 66:11	reconcile 73:18	regulatory 16:8	repeated 42:9
read 26:15 34:18 43:19 44:4 52:15 75:12	record 8:12 9:5 19:1 26:25 27:9 36:10 41:8 52:10 55:13 62:13 71:15,18 72:4,6 78:16,18	reidentify 49:2	rephrase 7:9,12 24:6 29:15
reading 37:3 61:17 66:8	records 9:6 14:13 22:18 23:16, 21 27:25 28:7,9,10,15 29:3,6,10,19 30:5,10 31:9,15 53:11 56:8,10 67:21 68:7,15,24 75:22 76:10	reidentifying 53:13	replies 9:23
reads 25:2 40:17 47:2	recover 33:20 48:13 67:12	related 54:20	reply 7:22 8:8,12,17,18,23 9:8,20,24 10:6 11:22 26:8 50:11 51:7 57:6,22 60:19 61:5,8 69:24
real-time 61:18	recoverable 65:4 72:9	relates 13:19 26:25 55:21	report 21:3,19 22:1,5,11 36:20,24
reason 7:2 37:10	recovering 65:14	relating 25:3	Reporter 6:3,4 68:19 78:15
reasonable 16:11,15,17	recovers 33:25	relationship 26:17	representation 12:19 57:17
recall 12:12 19:13 21:7 27:22 37:19 55:4	recovery 65:17	releases 53:11	representing 13:21 34:16
receive 29:19	refer 8:22 17:19 34:21 50:11 53:25 70:17	reliable 27:10 60:22	reproducible 52:21
received 20:1,20 29:5 30:9	reference 40:24 52:7 63:24 66:22 67:14	relies 60:24	request 18:17,20,25 19:1,3,15, 17,18,22 20:1,5,8,11, 13,15,17,20 21:1,4,8,22 22:4 33:9 34:13 35:9, 12,16 40:18 42:20,21 43:1,7,9,10,12,18,20,25 44:7,8,14,16,20 45:2,5, 11,17,24 46:7,10,13,17 70:9
receives 21:14	references 9:9 61:6	rely 27:11 60:11	requested 21:14 23:6 68:19
receiving 34:13	referring 8:23 24:2 59:17,19,22,	relying 60:10,17	
Recency 37:25		remains 72:1	
recently 8:9,18		remember 55:8 57:18	
		remote 21:11	
		remove 48:3	

THE SULLIVAN GROUP OF COURT REPORTERS

requests 42:15 44:18,22 78:16 require 38:3 54:15 65:7 required 52:6 requirement 44:11 54:24 55:3,6 58:12,15 59:5 61:10 65:1,11,20 72:10 requirements 14:20 15:13,17,25 16:4, 7,8,9,14,19 17:1,4,5,8, 16 25:3 51:5 54:12 Requires 43:3 resolution 74:3,18,19 75:16 76:7, 25 respect 19:14,19 respective 8:13 52:11 53:12 respond 63:14 responding 7:3 response 38:11 39:5 41:25 responses 41:22 restrict 36:23 restricted 36:19 restrictions 51:9 result 76:1 retrieving 33:21 returned 42:3 reversed 66:16	reversible 56:14 58:22 61:8,13,20 63:16 67:3,5,18 reversibly 49:12 review 10:24 22:14 77:20 reviewed 11:2 54:19 ridiculous 29:21 39:2 risk 23:14 28:21,23 29:18, 24,25 30:2 31:5,23,25 32:3 Rivest 66:23 roles 33:21 RSA 66:23 67:9 rule 14:17 15:7 25:7,10,13 40:17 41:3,14,16 42:19 43:12,20,22,24 44:5,23 50:23 53:20 62:6 65:7 72:12 rules 40:1 S safe 71:8,24 72:2,4,11 screen 55:23 64:13,16 search 42:14,20 43:1,7,20 56:22 67:23 68:4,24 69:7,16 76:2,3,15,16 searchable 69:14 searcher 68:22 76:15,18,22 77:1 searches 43:3,4	searching 33:21 68:14 73:13 75:10,17,25 section 25:2 53:10 55:20 58:4 secured 56:5 securely 53:12 security 15:14 26:22 37:5 41:6 53:2 54:11 59:2 64:21 seeking 41:19 sending 20:8,9 sends 20:6 21:2,4,19 sentence 12:3 22:25 40:16 47:1 50:16 57:8 58:2 59:17, 23 70:2 74:1 sentences 13:18 separate 38:10 separated 36:15 series 33:4 server 33:19 45:3 46:8,22 service 35:20,22,24,25 36:1,9, 14,19,23 37:10,15,21 session 6:13 set 8:2 13:8,21 17:1 34:15 45:18 61:14 Settimi 63:24 64:1 66:10 67:20 68:13 69:13 70:13,15 Settimi's 70:4	Shamir 66:23 share 12:23 shared 65:3 shed 38:22 short 7:7,16 64:7 shorthand 6:4 11:12 show 76:19 shown 21:10,11 shows 13:1 21:6,18,21 22:3 shut 9:15 side 18:4 significant 10:3 70:21 significantly 13:13 Similar 40:23 similarly 14:9 simplicity 8:16 simply 38:24 40:4 sites 21:11 sitting 19:13 29:16 38:19 skill 11:8,12,18 16:10 60:11, 24 Smith 30:20 Social
--	---	--	---

THE SULLIVAN GROUP OF COURT REPORTERS

26:22 53:1 64:21	31:22 34:2,6,8 44:12	suitable	tech
software	45:15 47:17,24 50:5,8,	58:11	16:1
65:22,25 66:6	10 52:10,13 55:13,17	support	technical
solely	59:16 68:16,20 71:21	60:19 63:1	16:19 55:20 56:1
62:1	77:19,23 78:1,8,12	supporting	techniques
sotto	stick	62:16	34:23 56:14
32:5	34:9	supports	technologist
sources	stop	62:14 63:2	16:18,24
60:24	42:5	sworn	technologists
speak	store	6:8	16:1
70:5	53:12	symmetric	telling
speakign	stored	48:20,23,24 49:17	62:8,20
32:5	32:22 67:20 68:6,17,21	56:17 59:15 61:12,19,	ten-minute
speaking	strike	23 62:9,17 67:11,16,17	34:3
55:2 76:19	20:23 21:13 25:13	symptoms	term
specific	58:21 65:20 69:23	37:25 39:15	11:11 24:17 33:2 34:20
12:7 72:12	string	system	terms
specifically	65:2 66:1	13:20 14:20,22 15:10,	35:1 38:25
32:4 40:10 66:10	strip	12,17,22,24,25 16:3,6,	testified
Specifications	72:5 76:4	19,25 17:5,10 22:12	6:8 55:5
54:1	stripped	23:1 29:13 30:21 31:21	testify
spend	76:1,9,11	39:18,22,23,25 40:1,7	7:2
10:5,21	stuff	41:10,12 42:12 43:16	testimony
spoken	13:1 70:14	44:10 48:2 51:4,22	29:16 61:17 78:3
78:5	subject	52:1,4 54:4 59:12,15	tests
sponsor	38:23 40:3 56:9	60:14 61:1,14 69:11,14	39:16
70:22	submit	75:20	text
stand	40:18	systems	25:7
13:11 14:2	submitted	14:15 39:20 40:10	theoretically
standard	7:22 8:1,4,9,18 61:5	41:19 56:5 60:25 63:3	62:5
24:22 36:12 37:12	78:18	70:7	things
started	subprovisions	T	14:7,11 16:3 19:4,8,25
11:21	54:10	taking	22:11
state	subsection	6:17	thinking
40:6	54:1,7,11,15	talk	25:21
statement	subset	32:4	third-party
49:9	32:6 44:3	talking	22:19 23:5,20 28:2
states	substance	33:6 58:11 74:16,21	30:14
50:17 57:8 58:3	78:3	Tamara	threat
statistically	substantially	6:3	16:2 42:2
29:9,12 48:12	40:19	target	threshold
Stephens	substantive	70:24	41:7,11
6:10,16,19,23 17:9	11:17	tasked	thresholding
23:13 28:19 29:22	sufficient	16:24	41:9,10
	72:21	teaches	
		73:13	

THE SULLIVAN GROUP OF COURT REPORTERS

Thursday 6:1 time 10:5,21 11:8 33:4 38:20,24 40:5,20 41:4, 16,24 42:5,6,22 49:14 63:13,15 70:13 78:13 times 7:7 63:21 timesheets 10:12 today 6:17 7:4,21 8:17,22 11:17 29:16 78:3 today's 6:25 10:16 token 20:20 28:25 29:1,2 46:6,8,11 68:3 70:4 76:6,11 tokenize 48:3 tokenized 46:18 tokens 20:9,17 21:1,4,8 29:4 32:15 33:1,6,9,13,20,25 45:7 69:7,9,16 70:9 top 25:1 70:2 topics 11:16 total 37:19 43:24 44:6,7,13 track 10:3 44:17,21 transcript 78:15,17 transformation 58:5 transforming 47:5 translated 54:18 transmission 45:6,12	transmits 45:2 transmitted 32:16 33:11,17 46:5 treatment 39:16 treatments 37:25 trouble 25:21 26:1 true 26:10 54:25 truthfully 7:3 turn 11:15,25 13:5,15 18:1 22:13 26:13 27:17 32:9 34:10 35:4 40:12 44:24 46:24 50:12 52:14 55:18 57:5,19,21 70:12 73:25 77:3 two-fish 67:15,16 types 42:2 Typically 77:8	18:23 22:8 37:2,14 understands 37:5 understood 7:13 37:3 73:12 undoubtedly 7:7 unique 30:25 52:21 unplugged 24:4 untrusted 45:9 useless 73:9,16,22 user 18:5,9 34:13 40:17 42:15,22 44:22 45:1 73:1 76:20,23,24 users 43:21 74:11 usual 49:19 uttered 30:2	32:5 W wanted 30:11 69:3 waste 38:19,24 wasting 40:5 week 78:19 window 9:14 word 56:24 words 9:25 30:2 work 10:3 16:1,2 24:21 48:23 works 16:22 50:6 write 51:8 70:3 written 9:2 wrong 18:13 wrote 9:23 13:18 50:17
	U unable 75:4 76:15 unattainable 47:10 unauthorized 47:16 73:1 74:11 76:20, 23,24 unavailable 66:21 72:7,15 73:5,6 74:12,15,24 76:2,5,6, 12,22 77:2 understand 6:24 7:8,21 11:6,18 12:4 35:22 36:5,6 37:6 38:7,13,15 39:6,12 54:9 59:19 63:5 66:8 73:22 understanding	V values 58:5 Venable 6:21 10:18,25 version 52:22 view 27:2 Vigilytics 6:18 12:4,6 14:8 70:7 violated 14:23 15:22 violating 14:17 15:3 violations 15:6 voce	Y years 63:3 Yesterday 10:20
			Z zip 12:15 45:20 76:9,16,19 Zoom 9:11 10:18