1 UNITED STATES PATENT AND TRADEMARK OFFICE

2 BEFORE THE PATENT TRIAL AND APPEAL BOARD

3 ---

4 DATAVANT, INC.,

5

6 Petitioner,

CERTIFIED COPY

7 v.

8 VIGILYTICS LLC,

9 Patent Owner.

10 ---

Cases:

11 IPR2024-00307 (US Patent No. 9,965,651)
IPR2024-00311 (US Patent No. 10,109,375)

12 IPR2024-00381 (US Patent No. 10,886,012)
IPR2024-00382 (US Patent No. 9,665,685)

13 ---

14

VIDEOCONFERENCE DEPOSITION OF

15

DR. PAUL CLARK

16

17 MARCH 20, 2025

18 Page 1 - 81 10:09 a.m. - 1:22 p.m. EST

19

20

REPORTED BY:

21 Tamara L. Houston
CA CSR No. 7244, RPR, CCRR No. 140

22 Job Number: J12600076

23 Ref. 25412-0021IP1
Ref. 25412-0024IP1

24

25

Exhibit 2009
Datavant v. Vigilytics
IPR2024-00382

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.

APPEARANCE OF COUNSEL:

On behalf of the Petitioner:

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

On behalf of the Patent Owner and Witness:

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

INDEX TO EXAMINATION

WITNESS: DR. PAUL CLARK

EXAMINATIONS PAGE

Mr. Stephens..... 6

QUESTIONS INSTRUCTED NOT TO ANSWER

Page Line

NONE

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.)

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

--o0o--

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

--o0o--

DR. PAUL CLARK,

called as a witness

was sworn and testified as follows:

--o0o--

EXAMINATION BY MR. STEPHENS:

Q. Good morning, Dr. Clark.

A. Morning.

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

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

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

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

BY MR. STEPHENS:

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

A. Yes.
Q. Is there any reason that you cannot testify truthfully and completely in responding to my questions today?
A. No.
Q. I'll do my best to phrase my questions clearly, but undoubtedly I'll fall short at times. If you ever don't understand the question or need me to repeat or rephrase a question, please let me know. Okay?
A. Yes.
Q. And if you don't ask me to repeat or rephrase a question, I'll assume that you understood the question. Is that fair?
A. Yes.
Q. I'll also need to take a short break every hour or so, and we'll -- we can further plan for a longer lunch break. If you ever need to take a break as well, just let me know. Okay?
A. Yes.
Q. Do you understand that we're here today regarding the reply declarations that you submitted in the IPRs on the '651, '375, '012, and '685 patents?
A. I do.
Q. And these are the second declarations that you

submitted in each of these proceedings. Correct?

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

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

A. Yes.

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

A. Yes.

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

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

A. Yes.

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

A. Yes.

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

A. Nothing open, no.

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

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

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

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

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

A. It will not.

Q. How did you prepare your reply declaration?

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

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

drafted by counsel?
A. As we've discussed before, I don't really keep track of that. I -- I did a significant amount of work drafting.
Q. And about how much time did you spend preparing the reply declarations in these proceedings?
A. Several hours.
Q. More than five hours?
A. I'm sure.
Q. Less than 15?
A. I don't know for sure. I haven't checked my timesheets.
Q. Are you aware of any errors in your declarations?
A. No. If I was, I would have fixed them.
Q. And how did you prepare for today's deposition?
A. I had a Zoom with counsel for Venable.
Q. When did that occur?
A. Yesterday.
Q. And about how much time did you spend preparing for the deposition?
A. Couple hours.
Q. Did you independently review any materials apart from your meeting with Venable?

A. Yes.
Q. Are there any materials that you reviewed that are not identified in the list of materials considered in your declarations?
A. No.
Q. And I understand that the opinions in your declarations are offered from the perspective of a person of ordinary skill in the art at the time of the claimed inventions; is that correct?
A. Yes.
Q. If I use the term "POSA" or "POSITA" as a shorthand for a person of ordinary skill in the art, will you know what I mean?
A. Yes.
Q. All right. Great. I would like to turn to several topics; but as we do, I'd ask that you answer the substantive questions today from the perspective of a person of skill in the art as you understand it. Okay?
A. I'll do my best.
Q. All right. Let's get started.
So if you could open your reply declaration in the '651 patent, please.
A. Okay.
Q. And turn to paragraph 7.

Are you there?
A. Okay.
Q. The fourth line down, the sentence that begins, "I also understand that Vigilytics has generally agreed with definition of a POSA in my prior declaration; however, Vigilytics asserts that the POSA would have had specific knowledge about medical databases and the manner of operating the same to comply with HIPAA."
Do you see that?
A. Yes.
Q. Do you recall how you defined a POSA in your prior declaration?
A. Not from memory, no.
Q. And in the zip file I sent through the chat, I put in a copy of your first declaration in the '651 IPR proceeding.
Were you able to access that?
A. Or I can accept your representation as to what's in there. It's up to you.
Q. If you would open that, I think that would be -- I'd appreciate if you could follow along with me.
A. I'll try and get -- is this in the share?
Q. Yes.
A. Which button? Is that under docs or is it --

I don't know where that stuff shows up.
Q. Let me -- I'll put this individually into the chat. Might be easier.
A. Yeah.
Q. Okay. Once you have it open, I'll turn to paragraph 22.
A. Yep.
Q. This is where you set forth the definition for a POSA of the '651 patent.
A. Yes.
Q. And do you still stand by this definition of a POSA?
A. Sure. It's not, as I said, significantly different of the ones you guys have used.
Q. In the -- turn to paragraph 34 in this declaration, which is the background '651 patent.
A. Okay.
Q. And the first two sentences you wrote that, "The '651 patent relates to a computer-implemented system of producing information characterizing a group of individuals from a set of private data representing characteristics of individuals. De-identification is done in order to comply with the Health Insurance Portability and Accountability Act, HIPAA."
Do you see that?

A. That's what it says.
Q. And you stand by the accuracy of this explanation. Correct?
A. Yes.
Q. So the '651 patent is concerned with HIPAA compliance. Correct?
A. Among other things, yes.
Q. And the other four Vigilytics -- the other four patents at issue are similarly concerned with HIPAA compliance. Correct?
A. Yes, among other things.
Q. Why would a POSA implementing a medical records database be concerned with HIPAA compliance?
A. Because that's what governs the healthcare providers that they would be implementing systems for.
Q. A POSA would have been aware of penalties imposed by law for violating the HIPAA Privacy Rule. Correct?
A. I doubt that. They would have just seen them as system requirements for implementation.
Q. Are you aware of any penalties that could be incurred for knowingly implementing a system that violated HIPAA?
A. I'm not a lawyer. I would say that there would certainly -- if you were negligent, there would be

civil liability.

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

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

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

A. That's fine.

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

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

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

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

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

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

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

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

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

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

set of design requirements?

MR. OLIVER: Objection. Form.

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

BY MR. STEPHENS:

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

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

Q. And those are requirements under HIPAA. Correct?

A. Yes.

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

Do you have a copy of that patent?

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

Q. I can put it quickly in the chat.

A. Yep.

Q. All right. Turn to Figure 2, please, of the '651 patent.
A. Okay.
Q. And at the right side of Figure 2, there is a user or indicator of the hospital 150.
Do you see that?
A. Yes.
Q. Fair to say there's a beta flow that loops from the user through a third party 205, through a data aggregator 206; then through a data processor 210, and then back to the hospital 150.
Do you see that?
A. Well, I was on actually the wrong figure.
Q. I'm on Figure 2.
A. Yeah, I was cleverly on Figure 1. Let's see -- yes, I see that.
Q. So the hospital 150 sent a data request 203 to a third party 205. Correct?
A. Yep.
Q. What would be included in that data request 203?
A. I don't know. Well, anything.
Q. But I guess, based on your understanding of the '651 patent, what would be included in the data request?

A. It would be a request for a healthcare record.
Q. And are you familiar with what data would be included in the request?
A. I -- it could be any number of things.
Q. Such as?
A. I didn't hear your question.
Q. I'm sorry. You said it could be any number of things, and I was asking, "Such as?" Can you provide an example?
A. Yeah. Maybe a previous health condition, maybe, you know, current allergies. I mean, I don't know. Any -- anything.
Q. And sitting hear right now, do you recall what the '651 patent describes with respect to the data request?
A. Not from memory, no.
Q. Would the data request include a request for a group of individuals -- a request for healthcare information with respect to a group of individuals?
A. Certainly could.
Q. And how would the individual be identified in the data request?
A. I would have to look to the patent to see what examples they give. But, again, it could be any number of things.

Q. Okay. So the data request 203 is received by a third party 205. Correct?
A. Yes.
Q. And what does the third party 205 then do with that data request?
A. Sends it to a data aggregator.
Q. Does it perform any processing on the data request before sending to the data aggregator?
A. Since it's sending tokens, according to this embodiment, which is what the figure indicates, it would have de-identified that data request.
Q. And can you explain what you mean by de-identified the data request?
A. Yeah. It would have removed the PII from the data request.
Q. That's how the '651 patent describes creating request tokens by de-identification?
A. I believe so. I can look in the patent and see what else it says, if you wish.
Q. So the request token 204 is received by the data aggregator 206. Correct?
A. In this embodiment, yes.
Q. And what's -- what is the function -- strike that.
What does the data aggregator 206 do with the

request tokens?

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

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

A. That's what the figure shows.

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

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

Q. And what would that -- strike that.

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

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

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

A. That's what Figure 2 shows.

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

A. Yes.

Q. And then the data processor provides a report 212 to the hospital 150 as we just discussed. Correct?
A. In this embodiment, that's what it shows, yes.
Q. And is there a difference between the request of the de-identified data 208 and the report 212?
A. If it goes through a data processor, I would assume so.
Q. Based on your understanding, what would be the difference between those two?
A. Guessing at least formatting to generate the report, but any number of things could change depending upon the way you implement the system.
Q. Let's turn to Column 5 at line 34.
If you would like to take a moment to review that paragraph, please feel free.
A. Yes, I see.
Q. That line, 34 through 37, the patent explains that, "De-Identified data records may be provided to the data processor 210 (e.g., a third-party data processor), but that third party may not have access to any personally identifiable information 118 about the group 154."
Correct?
A. That's what it says.
Q. And then the last sentence of that paragraph

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

Correct?

A. That's what it says.

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

MR. OLIVER: Objection. Form. Foundation.

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

BY MR. STEPHENS:

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

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

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

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

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

(Interruption.)

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

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

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

Q. So PII is personally identifying information. Correct?

A. Yes.

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

A. That's correct. They overlap.

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

A. Yes.

Q. And what is that?

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

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

A. All right.

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

A. Yes.

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

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

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

A. Yes.

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

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

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

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

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

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

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

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

A. Can I close the other HIPAA one?

Q. Yes, you may.

A. Okay. Got it.

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

A. I believe that's true.

Q. What is Exhibit 1016?

A. Guidance -- HIPAA guidance from HHS.

Q. Turn to page 5.

A. Okay.

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

A. I see what it says.

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

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

So their guidance is flawed.

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

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

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

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

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

A. Because it's incomplete.

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

A. Okay.

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

Do you recall that?

A. Yes.

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

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

Correct?

A. That's what it says.

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

A. In this embodiment, yes.

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

MR. OLIVER: Objection. Form.

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

BY MR. STEPHENS:

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

A. Yes.

Q. And what is the re-identification risk?

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

Q. From what token?
A. From the de-identification token.
Q. From the de-identified data records?
A. Which are identified by tokens.
Q. Okay. So the data processor 210 received the de-identified data records for the individuals in the group. Correct?
A. Yes.
Q. And statistically, there's some possibility of re-identification from the de-identified data records. Correct?
A. No. Not statistically. It depends upon how the system is implemented.
Q. If you knew the individuals -- the identities of the individuals in the group -- I'll rephrase this.
Is it your testimony, just sitting here today, that the '651 patent was not concerned with the re-identification risk if the data processor were to receive the PII and the de-identified data records?
MR. OLIVER: Objection. Form.
THE WITNESS: That's ridiculous.
BY MR. STEPHENS:
Q. Well, I asked you earlier -- I asked what was the risk, and you said there was no re-identification risk.

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

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

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

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

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

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

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

Q. And why would you not do that?

A. Because I would not want someone with a unique

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

Q. That would be a re-identification risk?

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

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

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

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

MR. OLIVER: Objection. Mischaracterizes.

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

BY MR. STEPHENS:

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

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

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

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

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

A. Okay.

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

A. Okay.

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

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

Q. What is a batch file?

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

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

Is a batch file a file that contains the

individual tokens?

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

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

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

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

A. That's what it says.

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

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

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

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

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

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

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

THE WITNESS: That's fine.

MR. OLIVER: Okay.

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

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

BY MR. STEPHENS:

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

A. Okay.

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

Did I read that correctly?

A. Yes.

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

A. It says plain English meaning.

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

A. I believe so.

Q. Are the terms "pre- and post-encounter" terms of art in the '651 patent?
A. As I said, plain English meaning.
Q. Turn to Column 6, please.
A. Okay.
Q. I'll look at a paragraph that begins at line 6 through line 28.
A. Okay.
Q. And this paragraph refers to a request message 306. Correct?
A. Yes.
Q. The request message can include identifying data 404 for a group of individuals. Correct?
A. That's what it says.
Q. And then there is also nonidentified data 405 associated with the request message 306. Correct?
A. Yes.
Q. And at nine, identified data 405 is for pre-encounter and/or post-encounter details such as service dates or diagnosis information. Correct?
A. That's what it says.
Q. What would a POSITA understand a service date to be?
A. Plain English, the date of service.
Q. Of what service?

A. Healthcare service.
Q. Could it be a discharge date?
A. Any date associated with healthcare, I would think.
Q. Likewise, how would a POSITA understand -- or what would a POSITA understand diagnosis information to be?
A. Plain English meaning.
Q. And a service date and diagnosis information from the medical record would be protected health information under HIPAA. Correct?
A. I would have to look at the standard, but I would think so.
Q. As described in this paragraph, the service date for diagnosis information are separated from the PII 404 to create nonidentified data 405. Correct?
A. In this embodiment, yes.
Q. And the patent explains that access to the service date or nonidentified data 405 is restricted only to the report generator 328. Correct?
A. That's what it says.
Q. Why does the patent implement measures to restrict access to the service date or the nonidentified data, only to the report generator?
A. I don't know. I don't have it memorized, the

patent, where it may or may not explain that.

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

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

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

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

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

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

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

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

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

A. Recency of different treatments or symptoms,

it is useful information.

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

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

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

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

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

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

Q. And what is it?

A. Plain English meaning.

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

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

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

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

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

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

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

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

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

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

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

A. An expert system does analysis based upon

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

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

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

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

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

A. Yes.

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

A. That's what it says.

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

A. Yes.

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

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

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

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

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

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

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

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

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

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

Do you see that?

A. I do.

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

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

Q. And this analysis would involve a comparison

of the individuals identified by each search request. Correct?

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

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

A. In this example, yes.

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

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

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

A. Yeah. If we read it literally, which says, "any previous search request," then this rule would be invoked. An example that involves hundreds of users, I'm note sure that's the way I would implement the rule, but in this example that's correct.

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

Correct?

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

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

MR. OLIVER: Objection.

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

BY MR. STEPHENS:

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

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

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

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

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

A. Okay.

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

A. Yes.

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

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

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

MR. OLIVER: Objection. Form.

THE WITNESS: That's what it says.

BY MR. STEPHENS:

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

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

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

although in encrypted form. Correct?

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

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

A. That's correct.

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

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

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

A. In this embodiment, yes.

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

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

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

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

Q. Turn to Column 4, please.

A. Okay.

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

Do you see that?

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

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

MR. OLIVER: Objection. Foundation. Mischaracterizes.

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

BY MR. STEPHENS:

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

MR. OLIVER: Objection.

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

BY MR. STEPHENS:

Q. You agree that the irreversibly de-identified

data 140 would be absent PII. Correct?

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

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

A. If it's done properly, yes.

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

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

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

A. Yes.

Q. Can you give me an example?

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

Q. How does the symmetric cipher work?

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

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

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

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

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

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

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

A. That is correct.

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

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

A. No.

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

THE WITNESS: That's fine.

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

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

BY MR. STEPHENS:

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

Are you there?

A. Not yet.

Okay.

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

Correct?

A. That's what it says.

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

A. I would think so.

Q. Would HIPAA compliance be important for

consideration to a POSITA?

A. In this case, yes.

Q. Why is that?

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

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

Correct?

A. That's what it says.

Q. So Dick was also concerned with HIPAA compliance?

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

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

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

Q. And likewise, would a POSITA be interested in

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

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

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

A. I do.

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

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

THE WITNESS: Okay.

BY MR. STEPHENS:

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

A. Okay.

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

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

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

A. Yes.

Q. And that patient identifying information, some

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

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

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

A. In this embodiment, yes.

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

A. Okay.

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

A. In this embodiment, yes.

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

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

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

Do you still have a copy of that available?

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

Okay.

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

subsection C, Implementation Specifications: Re-identification.

A. Okay.

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

A. That's the way I understand it.

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

A. Yes.

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

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

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

A. That's what it said.

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

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

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

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

MR. OLIVER: Objection. Foundation.

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

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

THE WITNESS: Yes.

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

BY MR. STEPHENS:

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

Do you see that?

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

Okay. So you said Column 1.

Q. Column 1, line 14, under the "Technical Field of the Invention."
A. I see it.
Q. In this paragraph it describes how -- "to systems and methods that implement the secured key encryption for de-identifying patient data to ensure patient privacy, while allowing only the owners of the patient data records and/or other legally empowered entities to re-identify subject patients of de-identified data records when needed."
Correct?
A. That's what it says.
Q. And to allow for re-identification, Landi uses reversible encryption techniques. Correct?
A. In the embodiment we were discussing, it was using public key, but, yes, that's -- I -- normally not what you would use for a symmetric cipher would be the preferred mode, but, yes.
Q. And Landi never describes caching PII through forming encrypted ID; is that correct?
A. Caching? I don't have complete recollection, but I can search it for hash, if you wish.
Q. Yes, please.
A. The word "hash" does not appear in Landi.
Q. And if the PII were hashed to form the

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

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

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

A. Okay.

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

A. Yes.

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

A. Yes.

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

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

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

A. Okay.

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

A. Yes.

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

A. Yes.

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

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

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

A. That's what it says.

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

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

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

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

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

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

MR. OLIVER: Object. Form.

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

BY MR. STEPHENS:

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

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

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

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

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

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

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

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

A. It is cited, yes.

Q. Do you believe that this guidance is reliable?

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

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

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

A. I cited to these references, yes.

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

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

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

A. That's correct.

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

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

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

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

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

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

A. Yeah, my CV.

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

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

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

declaration that support that position. Correct?

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

Q. I'll just give you one last opportunity.

Is there any --

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

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

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

A. Asked and answered.

Q. Are you refusing to answer?

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

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

Do you have a copy of Settimi available?
A. I do.
Q. Let's look at paragraph 41, please.
A. Yes.
Q. This paragraph describes methods for generating an encoded patient identifier, or EPID for short. Correct?
A. Yes.
Q. That EPID can be generated by a patient care provider, or PCP. Correct?
A. Yes.
Q. And this paragraph describes how EPID can be generated from, say, a password screen and identifying information for a patient. Correct?
A. In this embodiment, yes.
Q. That password screen is known only to the PCP. Correct?
A. Yes.
Q. And the identifying information can be, for example, a patient identifier or other information such as patient name, age, and Social Security number. Correct?
A. Correct.
Q. And so if the identifying information is not hashed, it would fail to comply with the derivation

requirement. Correct?

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

Q. That wasn't my question.

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

A. Not according to --

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

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

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

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

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

A. That's what it says.

Q. And it says that that software hashes the

encoded password string to produce a 16-digit number. Correct?

A. It does.

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

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

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

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

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

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

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

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

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

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

we were discussing previously.

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

A. Not without access to the private key.

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

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

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

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

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

A. Two-fish is a symmetric algorithm.

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

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

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

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

Q. Would that have been an important

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

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

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

MR. OLIVER: Objection. Mischaracterizes. Foundation.

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

BY MR. STEPHENS:

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

(Court Reporter requested clarification.)

BY MR. STEPHENS:

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

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

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

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

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

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

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

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

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

A. It is.

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

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

A. Okay.
Q. At the top of page 10, the last sentence you write that, "Evenhaim's query would be formatted to match the token designed used by Settimi's database so that they speak the same language," correct?
A. At paragraph 12? Yes, I see it.
Q. Do you have any systems before the Vigilytics patent in which a third party encrypted PII to generate request tokens that could be matched against a de-identified dataset?
A. Not from memory.
Q. Okay. Let's turn to Evenhaim, please.
A. May I close Settimi? I'm having a hard time getting through all this stuff on my desktop.
Q. Yeah. Please go ahead and close Settimi.
A. Okay. I have it up.
Q. And I'll refer to the -- there's a paragraph in Column 4 at lines 34 to 48.
A. Okay.
Q. And in this paragraph, Evenhaim identifies a significant challenge with measuring the impact of a consumer health program when the health program sponsor does not have the full healthcare information of the target population at their disposal. Correct?
A. That's what it says.

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

Do you see that?

A. Yes.

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

A. Yes.

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

A. Yes.

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

MR. OLIVER: Objection. Form.

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

BY MR. STEPHENS:

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

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

A. And my answer remains the same.

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

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

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

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

A. Right. They must be unavailable.

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

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

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

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

unauthorized user, yes.

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

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

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

A. That's what it says.

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

A. No. I don't think so.

Q. What does "useless" mean to you?

A. Plain English meaning.

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

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

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

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

A. Yes. That's what it says.

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

A. Not necessarily, no.

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

A. To unauthorized users, that's correct.

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

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

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

In that instance, the information would be

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

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

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

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

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

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

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

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

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

A. Yes.

Q. And when searching that database, the

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

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

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

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

Q. Either way. Okay?

A. Yeah, I'm listening.

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

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

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

A. To the unauthorized user, yes.

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

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

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

Do you see that?

A. I do.

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

A. That's what it says.

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

A. That means to agree to participate.

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

A. I would expect so.

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

THE WITNESS: Okay.

MR. STEPHENS: Thanks.

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

BY MR. STEPHENS:

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

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

Q. Anyone else?

A. Nope.

MR. STEPHENS: All right. No further questions.

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

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

THE WITNESS: All right. Thank you.

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

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

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

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_____

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

STATE OF CALIFORNIA))) ss.

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

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

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

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

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

In witness whereof, I have hereunto subscribed my name.

Dated: 24th of March, 2025.

Tamara L. Houston

TAMARA L. HOUSTON
CSR 7244, RPR, CCRR 140

-

--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,

19 40:16 52:14 77:3

500
43:10

56
53:8

6

6
35:4,6 45:16 53:7

64
73:25

65
53:8

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

685
7:23

7

7
11:25 45:10 52:14

700
43:11

7244
6:4

8

8
32:9

9

9
40:12 42:10

A

a.m.
6:1 34:7 50:9 55:16

abide
54:7

ability
62:17

absent
48:1

accept
12:19 57:17

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

accompanied
8:5

account
42:6

Accountability
13:24

accuracy
14:2

acknowledge
73:19

acknowledges
51:9

acquiring
52:1

Act
13:24

additional
41:20

address
53:2

addresses
27:6

Adelman
66:23

age
64:21

aggregator
18:10 20:6,8,21,25 21:8,15 69:20

agnostic
75:17,19

agree
16:23 45:5 47:18,25 77:14

agreed
12:5 74:8

agreeing
77:15

agreement
30:12

ahead
70:15

aimed
16:17

algorithm
57:4 63:16 66:23,25 67:2,3,12,15,16,17,18

allergies
19:11

allowed
23:24

allowing
53:16 56:7

ambiguity
59:21

amount
10:3

Anaheim
75:9

analyses
34:24

analysis
37:16,24 38:2,7,14,16 39:7,13,17,19,25 40:2 42:25 60:19

analyze
74:2 75:2

analyzed
74:13

and/or
35:19 51:6 53:2 56:8

anticipated
23:23

appearance
6:20

appears
41:25

applied
48:16

applies
60:4

apply
39:8 58:17 72:18 74:5

argue
55:2

art
11:8,12,18 33:3 35:2 60:25

asserts
12:6

assigned
54:4

assume
7:13 15:5 22:7 46:4 74:21

assurance
72:21

attached
48:13

attacker
42:8

attainable
46:16 47:19,23

attempts
42:5

auditing
43:3

authority
60:7

authorized
71:19 74:14,23 75:8

authorizing
77:16

aware
10:13 14:16,21 15:2 60:7

B

back
18:11 21:20 27:17 34:6

42:10 50:8 51:7 55:18 57:5

background
13:16

based
18:23 22:8 32:1 37:2 39:25 42:20 59:20 61:18

basically
68:12

batch
32:16,20,21,23,25 33:2, 6,10,12,13,16,20,24

begins
12:4 26:16 32:11 35:6 40:13 57:24

behalf
6:17,22

beneath
55:19

benefits
51:9

beta
18:8

birth
45:20

bit
39:9

bits
59:2

breaching
31:23

break
7:16,18 34:3

breaks
78:2

bring
24:22

broader
25:17

building
52:4

built
51:4

business
23:12,24 30:6

button
12:25

C

caching
48:9,14 56:19,21

California
6:4

called
6:7 41:6

capable
54:17

care
64:9

case
15:9 33:5 49:1 51:2 65:17

cases
6:14

cautious
73:23

centralized
67:21 68:6,17,21,23 69:20 75:22

Certified
6:4

challenge
70:21

change
22:11

channel
45:8

channels
9:12

characteristics
13:22 34:16

characterization
26:21 27:13

characterizes
34:14

characterizing
13:20

charged
16:24

chat
12:15 13:3 17:24 24:24 26:4

check
44:15

checked
10:11

checks
42:12

cipher
48:23,24 49:10,16,17, 21,22 50:3 52:20 56:17 61:12,19,23 62:17

ciphers
48:20 62:9

circumstances
60:12

cite
57:12

cited
26:8 40:23 57:21 60:18, 21 61:6,7 62:25

civil
15:1,6,19,21

Claim
34:10,12 40:23 41:2

claimed
11:9

claims
21:11

clarification
68:19

clarify
71:22

clarity
39:5

Clark
6:6,11,24 9:1 28:21 34:9 39:3 60:16 63:12 78:2,13

class
49:15

clear
60:16 62:24 63:13

clearing
21:11

cleverly
18:15

close
26:5 70:13,15

closed
53:23

code
45:20 54:5 58:18 76:9, 16,19

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

combination
69:12,13,17 75:21

combined
55:3

communication
9:12

compare
43:4,6

compared
44:19

comparison
42:25

complete
56:21 59:20

completely
7:3

compliance
14:6,10,13 16:8 50:19, 22,25 51:15,20 54:8 63:17 72:14

compliant
30:11 31:12 51:22 55:6 60:8 62:6,18 71:20 73:2

complied
15:17

comply
12:8 13:23 15:11 16:16 17:12 52:2 54:23 60:12

61:15 62:10,21 64:25 65:10 66:8

complying
16:18

composed
34:14

comprising
34:13

computationally
48:12

computer-implemented
13:19 34:12

concept
28:20 37:6 41:6

concerned
14:5,9,13 15:18 29:17 51:14

concluded
78:20

condition
19:10 30:18 31:2

conditions
31:19

confirm
9:14

confirms
45:10

consideration
51:1 68:1

considered
11:3 67:9

constitute
26:20

construct
49:16 62:1

constructed
67:12

constructing
49:21

consumer
70:22

consumers
77:9

contemplates
51:10,17

contention
68:22

context
32:23 76:21

continuing
40:19

copies
9:5

copy
12:16 17:21 52:7 53:22 64:1 78:19

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

correctly
34:18

counsel
6:19 9:12 10:1,18 78:4, 5,15

Counselor
38:20 49:14 62:20 63:10

countermeasures
16:12,16,17 17:14

Couple
10:23

court
6:3 68:19 78:15

covered
23:11,23 26:3 30:6,8,9, 13 31:20 54:6

create
33:8 36:16 48:21 49:8 58:18

creating
20:16 33:13

criminal
15:2,6,19,21

criticizes
73:19

cryptographic
48:11,14 49:7,10,18 58:6 59:2,6,25 62:1 63:3 65:16 66:7

cryptography
49:15

current
19:11 43:5

CV
9:10 62:15 63:7,21

D

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 75:2 76:10,21

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

databases
12:8

dataset
70:10 72:22,24 73:3,4 74:3,6,9,10,20 75:3 76:25

datasets
75:10,14,15,18 76:9

Datavant
6:22

date
35:22,24 36:2,3,9,15, 19,23 37:10,15,21 38:3 45:20

dates
35:20

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

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

de-identifier
47:2

de-identify
16:11 51:6 72:4 74:19

de-identifying
27:8 56:6

dealing
41:11

dec
9:23 57:22

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

64:6 66:1

encoding
65:22 66:6,7

encompass
16:8

encounter
38:4 39:15

encounters
41:7

encrypt
45:7,8 48:25 49:19 57:9

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

encrypting
33:6,10 76:5

encryption
45:2 46:8,22 48:15 49:3 56:6,14 58:23 61:8 63:16 67:3,18

encrypts
33:8 75:2

English
34:22 35:3,24 36:8 37:20 38:18,21,25 39:8, 10,17 73:17

ensure
56:6

entire
74:18

entities
56:9 61:2

entity
23:12,24 30:6,9,13 31:16,20 53:11,17 54:6 74:22 75:1

EPID
64:6,9,12 66:10,13,18 68:6,15

EPIDS
67:20 68:17,21,23

errors
10:13

EST
34:7 50:9 55:16 77:24

Evenhaim
69:15 70:12,20 73:7,13, 19 74:18 75:13,17 77:8

Evenhaim's
69:19 70:3

Evenhaim/settimi
68:1,5 69:11 75:21

evidence
27:10 62:13

EXAMINATION
6:10

examine
62:20

examples
19:24 25:25 26:19 45:22 53:1

exceptions
58:14 59:5

excuse
27:25 49:25 63:12

executed
32:22 33:3

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

exhibits
9:8

existing
73:8

expect
51:20 77:18

expert
39:20,21,23,25 40:7,9 49:25 58:6 60:1 71:9,24 72:16,17,19,23

expertise
63:6

explain
20:12 23:19 25:15 37:1 39:23 41:8

explained
23:22

explains
22:17 23:1 32:15 36:18 45:17 58:16 73:7 77:8

explanation
14:3 59:24

explicit
67:23

explicitly
50:17 51:16 57:9

express
62:25 75:13

expresses
75:9,15

extent
71:13

F

face
15:20,21

facility
34:17,21 38:4

fact
33:5 46:21 63:4

fail
64:25

failed
42:4

fails
15:11

fair
7:14 18:8

fall
7:7

familiar
15:4 17:4 19:2 24:7 28:20 71:5

features
23:1 40:23 51:21 52:1,6

feed
9:11

feel
22:15

field
50:1 55:20 56:1

figure
18:1,4,13,14,15 20:10 21:6,10,21 32:19 44:24 45:1 52:19

file
12:15 32:16,20,21,22, 24,25 33:2,7,10,12,14, 16,20,24 52:3

files
9:6

finally
21:19

find
67:23

fine
15:8 34:4 50:7

fix
55:11

fixed
10:15

flawed
27:1,3,15

flow
18:8

focus
8:16

follow
12:22 39:5 62:8

form
17:2 23:9 28:16 29:20 45:13 46:1 56:25 59:11 63:6 71:16

formatted
70:3

formatting
22:10

forming
56:20

Foundation
23:9 47:12 55:7 68:10

fourth
6:13 12:3 51:8

free
22:15 75:6

frequency

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

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

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

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 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

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

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

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

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

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

quickly
17:24

quote
23:6 32:15

R

re-ask
24:5

re-identification
23:14 28:21,23 29:10, 18,24 30:1,16 31:5 54:2,5 56:13 58:3,18

re-identified
53:17 54:6 71:14

re-identify
28:14 30:21 53:19 56:9 66:11

read
26:15 34:18 43:19 44:4 52:15 75:12

reading
37:3 61:17 66:8

reads
25:2 40:17 47:2

real-time
61:18

reason
7:2 37:10

reasonable
16:11,15,17

recall
12:12 19:13 21:7 27:22 37:19 55:4

receive
29:19

received
20:1,20 29:5 30:9

receives
21:14

receiving
34:13

Recency
37:25

recently
8:9,18

recess
34:7 50:9 55:16 77:24

recipient
59:14 66:21 71:18

recipients
58:9 59:9

recognizes
32:3

recollection
56:21

recommend
31:7,8,11

reconcile
73:18

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

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

recover
33:20 48:13 67:12

recoverable
65:4 72:9

recovering
65:14

recovers
33:25

recovery
65:17

refer
8:22 17:19 34:21 50:11 53:25 70:17

reference
40:24 52:7 63:24 66:22 67:14

references
9:9 61:6

referring
8:23 24:2 59:17,19,22, 23,24 71:23

refers
24:14 34:12 35:9 41:2 71:1

refresh
25:14

refusing
63:19,20

regard
9:21 15:14,15

regulations
16:20

regulatory
16:8

reidentify
49:2

reidentifying
53:13

related
54:20

relates
13:19 26:25 55:21

relating
25:3

relationship
26:17

releases
53:11

reliable
27:10 60:22

relies
60:24

rely
27:11 60:11

relying
60:10,17

remains
72:1

remember
55:8 57:18

remote
21:11

remove
48:3

removed
20:14 71:12 72:13

removing
47:3

render
73:9,21 76:5,6

rendered
74:24

reopen
53:23

repeat
7:9,12

repeated
42:9

rephrase
7:9,12 24:6 29:15

replies
9:23

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

report
21:3,19 22:1,5,11 36:20,24

Reporter
6:3,4 68:19 78:15

representation
12:19 57:17

representing
13:21 34:16

reproducible
52:21

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

requested
21:14 23:6 68:19

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

26:22 53:1 64:21

software
65:22,25 66:6

solely
62:1

sotto
32:5

sources
60:24

speak
70:5

speakign
32:5

speaking
55:2 76:19

specific
12:7 72:12

specifically
32:4 40:10 66:10

Specifications
54:1

spend
10:5,21

spoken
78:5

sponsor
70:22

stand
13:11 14:2

standard
24:22 36:12 37:12

started
11:21

state
40:6

statement
49:9

states
50:17 57:8 58:3

statistically
29:9,12 48:12

Stephens
6:10,16,19,23 17:9 23:13 28:19 29:22 31:22 34:2,6,8 44:12 45:15 47:17,24 50:5,8, 10 52:10,13 55:13,17 59:16 68:16,20 71:21 77:19,23 78:1,8,12

stick
34:9

stop
42:5

store
53:12

stored
32:22 67:20 68:6,17,21

strike
20:23 21:13 25:13 58:21 65:20 69:23

string
65:2 66:1

strip
72:5 76:4

stripped
76:1,9,11

stuff
13:1 70:14

subject
38:23 40:3 56:9

submit
40:18

submitted
7:22 8:1,4,9,18 61:5 78:18

subprovisions
54:10

subsection
54:1,7,11,15

subset
32:6 44:3

substance
78:3

substantially
40:19

substantive
11:17

sufficient
72:21

suitable
58:11

support
60:19 63:1

supporting
62:16

supports
62:14 63:2

sworn
6:8

symmetric
48:20,23,24 49:17 56:17 59:15 61:12,19, 23 62:9,17 67:11,16,17

symptoms
37:25 39:15

system
13:20 14:20,22 15:10, 12,17,22,24,25 16:3,6, 19,25 17:5,10 22:12 23:1 29:13 30:21 31:21 39:18,22,23,25 40:1,7 41:10,12 42:12 43:16 44:10 48:2 51:4,22 52:1,4 54:4 59:12,15 60:14 61:1,14 69:11,14 75:20

systems
14:15 39:20 40:10 41:19 56:5 60:25 63:3 70:7

T

taking
6:17

talk
32:4

talking
33:6 58:11 74:16,21

Tamara
6:3

target
70:24

tasked
16:24

teaches
73:13

tech
16:1

technical
16:19 55:20 56:1

techniques
34:23 56:14

technologist
16:18,24

technologists
16:1

telling
62:8,20

ten-minute
34:3

term
11:11 24:17 33:2 34:20

terms
35:1 38:25

testified
6:8 55:5

testify
7:2

testimony
29:16 61:17 78:3

tests
39:16

text
25:7

theoretically
62:5

things
14:7,11 16:3 19:4,8,25 22:11

thinking
25:21

third-party
22:19 23:5,20 28:2 30:14

threat
16:2 42:2

threshold
41:7,11

thresholding
41:9,10

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

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
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

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
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

Y

years
63:3

Yesterday
10:20

Z

zip
12:15 45:20 76:9,16,19

Zoom
9:11 10:18