STATE OF ILLINOIS)
) SS:
COUNTY OF C O O K)

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS

COUNTY DEPARTMENT - CHANCERY DIVISION

GREGG BRUHN, individually and on behalf of all others similarly situated,	)	
Plaintiffs,	)	
vs.	)	No. 2018 CH 01737
NEW ALBERTSON'S, INC., CERBERUS CAPITAL MANAGEMENT, L.P., AB ACQUISITIONS, LLC, ALBERTSONS COMPANIES, LLC, and AMERICAN DRUG STORES, LLC,	)	
Defendants.	)	

TRANSCRIPT OF PROCEEDINGS at the motion in the above-entitled cause before THE HONORABLE ANNA M. LOFTUS, Judge of said Court, in Room 2410 of the Richard J. Daley Center, Chicago, Illinois, on Tuesday, July 2, 2019, at the hour of 10:30 a.m.

REPORTED BY:
ANDREW R. PITTS, CSR, RPR
LICENSE NO.: 084-4575

APPEARANCES:

STEPHAN ZOURAS, LLP, by
MR. JAMES B. ZOURAS
MR. ANDREW C. FIZCKO
205 North Michigan Avenue
Suite 2560
Chicago, Illinois 60601
312.233.1550
jzouras@stephanzouras.com
afizcko@@stephanzouras.com

Appeared on behalf of the Plaintiffs;

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP, by
MR. MARK S. EISEN
333 West Wacker Drive
Suite 1900
Chicago, Illinois 60606
312.212.4949
meisen@beneschlaw.com

Appeared on behalf of the Defendants.

(WHEREUPON, the following proceedings were had in open court.)

THE CLERK: 10:30 status hearing. 18 CH 1737, Bruhn v. Albertson's, Inc.

THE COURT: Good morning -- afternoon -- yes, we are still on morning.

MR. ZOURAS: Good morning, your Honor. Jim Zouras for the Plaintiff.

MR. FICZKO: Good morning, your Honor. Andy Fizcko on behalf of Plaintiff.

THE COURT: Okay.

MR. EISEN: Mark Eisen on behalf of Defendants.

THE COURT: All right. This is Defendants' 2-619.1 combined motion to dismiss. If you would like to begin.

MR. EISEN: Thank you, your Honor. As I think the Court indicated in the last hearing we had, this is simply a matter of statutory interpretation, and that is whether the BIPA's exemption for information collected from the patient or information collected, used, and stored for health care treatment, payment, and operations means what it says, and that is that the statute creates two exceptions: One for patient

information and the second for information captured collected, used, for treatment, payment, and operations.

This is a very straightforward question, and this question can be addressed on the basis of the complaint alone. Plaintiff admits that he used the biometric authentication to access the pharmacy computer system. That is the only thing Plaintiff used the biometric identification to do.

And it is undisputed that a pharmacy like Jewel-Osco is a covered entity under HIPAA, that patient data is protected health information under HIPAA and that, as Plaintiff admits in their opposition brief, biometric authentication is a means of complying with the HIPAA's requirement for a technical safeguard to access pharmacy --

THE COURT: So HIPAA doesn't protect the pharmacist's biometric information.

MR. EISEN: I'm sorry.

THE COURT: HIPAA doesn't protect the biometric information of the pharmacist.

MR. EISEN: HIPAA speaks to --

THE COURT: It just addresses the patient records that are within that system.

MR. EISEN: Correct. And I think that in a very pertinent way, it does also speak to the records of an employee like a pharmacist or a doctor.

THE COURT: How so?

MR. EISEN: HIPAA speaks to protecting patient information.

THE COURT: Patient.

MR. EISEN: Right. Right, but I think the key focus is also on what HIPAA is intended to do is to protect. And in order to protect, HIPAA requires technical safeguards to access protected health information.

THE COURT: But are there provisions within HIPAA that state a provider's, in this case a pharmacist's, biometric information that is used in the fashion of securing the protected HIPAA information is also safeguarded under HIPAA?

MR. EISEN: HIPAA itself does not speak to that in those words, but BIPA doesn't require it.

THE COURT: I am not saying that it did.

MR. EISEN: Sure.

THE COURT: I am just making that point. Okay.

MR. EISEN: Right. And I appreciate that point

because I think it is important to recognize that what BIPA speaks to in this context is information collected, used, and stored for health care treatment, payment, and operations, and it is, I think, inconceivable to think that patient biometric information could ever been collected, used, or stored, for example, for payment.

THE COURT: I'm sorry?

MR. EISEN: So the statute exempts information collected, used, and stored for health care treatment, payment, or operations under HIPAA, and I think it is difficult to envision a scenario in which a patient's biometric information would be collected for payment. And the most common reading --

THE COURT: It might be used or stored for payment because there might be a -- what is the code, the CPT code or the code that they have to use for payment? They have to confirm that a scan was done, for instance.

MR. EISEN: That may be, but I think the definitions that HIPAA uses for payment, treatment, and operations are all focused on the covered entity. These aren't patient-focused definitions,

those definitions which we recited in our reply.

THE COURT: Well, it's the health care treatment of the patient, the payment for the health care treatment that the patient obtained, and then operations of the health care facility is what I got from your brief.

MR. EISEN: Right. And those definitions -- I think, treatment is the provision, coordination, or management of health care and related services by a health care provider. That is a covered-entity-focused definition. Health care operations, as the Department of Health and Human Services effectively says, is activities necessary to supported the core functions of the covered entity of treatment and payment.

And these are definitions that are focused on what the covered entity needs to do. And since at least 2003, HIPAA has specifically required a technical safeguard in order to access patient information, protected patient information. And one --

THE COURT: So are you saying that if the pharmacy in this case chose biometric information, then that information somehow brings everything

under HIPAA but not BIPA?

MR. EISEN: I'm sorry. I am missing that.

THE COURT: So you said that HIPAA requires technical safeguards.

MR. EISEN: Correct.

THE COURT: Okay. And one of those, the options, is biometric information.

MR. EISEN: Correct.

THE COURT: So how is that relevant to this argument?

MR. EISEN: The BIPA-exempt biometric information collected, used, and stored for treatment, payment, or operations under HIPAA, this is biometric information collected, used, or stored for both treatment and in order to access the pharmacy database to prescribe medication, to access the pharmacy database to effectuate payment. To allow for health care operations, the fundamental goal of HIPAA to protect that health care information, that is the only purpose this authentication safeguard has been enacted.

I think it is beyond question that HIPAA would require, does require, a technical safeguard on the pharmacy database, and that is undisputed.

The only real dispute Plaintiff's counsel seems to have is the methods chosen.

THE COURT: So I see you are saying that because it requires a technical safeguard, one of which is biometric identifiers, that that means that Section 14-4/10, the second phrase in the first sentence applies to that.

MR. EISEN: Correct. Correct. And that --

THE COURT: And that is based on just the fact that there is a provision in HIPAA that says you need to have a technical safeguard, and then this sentence, you are arguing, applies because they collect, use, and store the biometric information of the pharmacist?

MR. EISEN: Correct. This section -- and I think read in conjunction also with the statute of exemptions, which is at Section 25 of the statute, that says nothing in this statute should be read to conflict with HIPAA. And, again, the fundamental purpose of HIPAA is to protect patient information, and the means used to secure that patient information falls well within the structures of HIPAA.

THE COURT: Patient information, yes, but we

are still talking about a pharmacist's fingerprint, which is not part of the patient record. It is not the patient information that is obtained on the computer system. You are lumping them all in as one, I see, and I see your argument as to how they do that. And I think counsel is going to state the opposite, obviously.

MR. EISEN: Right.

THE COURT: How does the Plaintiff's positions conflict with HIPAA?

MR. EISEN: Well, at first, to answer the Plaintiff's --

THE COURT: If you are arguing it does.

MR. EISEN: Right. Well, Plaintiff's, I think, first argument conflicts with the plain language of the statute itself, which exempts patient information or information collected, used, and stored for health care treatment, payment, or operation.

THE COURT: So it is your position that Section 10 is ambiguous?

MR. EISEN: It is not ambiguous. Our position is that it is not ambiguous. It protects patient information, one, or, two, information collected

used, and stored for treatment, payment, or operations.

The first speaks only to patient information, and if the second were also to be limited solely to patient information and the second aspect of that sentence would be superfluous.

THE COURT: Well, now, you recently said that patient information isn't necessarily needed for payment or operations or something to that effect. So wouldn't that go against your argument then, that that second piece -- I think you previously said, if I'm not mistaken, that the second portion of this sentence, information collected, used, or stored for health care treatment, payment, or operations did not have much to do with patient information, and that is why it is reasonable to have two different exclusions in that one sentence.

MR. EISEN: Correct.

THE COURT: Correct? Okay.

MR. EISEN: Because if, as Plaintiff's counsel suggests, that second clause should also only pertain to patient information, well, that's already covered by the first clause. There would be no need for the second clause if it was only to apply to

patient information.

And I think a clear example for why this language must be read to include the health care provider in this context, the pharmacist as well, is as Plaintiff suggested in their opposition, 'Well, this language is really only intended for,' let's say, 'an optometrist needing to do a retinal scan. Well, the patient shouldn't be able to sue the optomotrist.'

But it would be, I think, anomalous to say that while the patient can't sue the optometrist, the optometrist which then goes and stores the scan on a computer can sue the computer provider because it didn't obtain biometric authorization, BIPA consent, to access the data.

THE COURT: From the patient?

MR. EISEN: From the physician.

THE COURT: For his fingerprint, for instance?

MR. EISEN: Right. Right. And HIPAA requires a technical safeguard to access patient information. And to say that the patient can't sue over the scan, but then the physician can then sue --

THE COURT: For the separately -- I think we have already established that HIPAA doesn't protect

his biometric information specifically.

MR. EISEN: Right, but it --

THE COURT: So that is where BIPA comes in and would say, 'Hey, we are going to also provide some protection for this. He needs to be told' -- a physician or an optometrist needs to be told that his fingerprint is being used and all of these other things.

MR. EISEN: The way the exception is phrased is to avoid the BIPA imposing extra requirements or running head on to HIPAA. And so the two statutes need to be read, I think, in unison, that while HIPAA does speak to patient information, the key aspect of HIPAA is in protecting the patient information.

So whatever is done, the Department of Health and Human Services has a long record of using biometric authentication. That is information collected, used, or stored to comply with HIPAA.

And the focal point, I think, the take-away from HIPAA is in protection. And in order to effectuate that purpose, a pharmacy needs to be able to implement a biometric authentication if it so chooses. And there are, I think, various other

types of authentication which have historically proven not to work as well, and we have had data breaches and the like, but the --

THE COURT: So if a pharmacy chose a different security method that didn't involve biometric information, it could still comply with HIPAA, but BIPA doesn't come into play?

MR. EISEN: Correct. The language of the security rule does not require a biometric authentication, but, as Plaintiff's counsel, I think, accepted in their opposition brief, it is an acceptable means to comply with HIPAA.

And what the BIPA, by this exception exemption and by the exemption located in Section 25 about not being read to conflict with HIPAA, well, I think the two statutes need to be read together such that if a health care provider, whether it be a pharmacy, a hospital, doctor, if they choose, this is how we are going to comply with HIPAA, and this is a requirement. We have to implement a technical safeguard. We cannot be punished for the safeguard we implemented, nor should we look to -- it would be --

THE COURT: How are they punished for the

safeguard that they choose in that scenario?

MR. EISEN: This statute or any other state statute would require extra measures on top of what the pharmacy has chosen to implement or on top of what the hospital has chosen to implement as their best means of complying with HIPAA and protecting that patient information, that I think tend to be -- you could certainly envision a scenario where if a pharmacist were to opt out and say, 'I don't want to do that; I want to use some other perhaps less safe mechanism to comply,' this is something that puts patient information at risk.

And if a pharmacist or a hospital or a physician's group determines this is the best way to protect patient information, that is all that the statute requires.

THE COURT: Which statute?

MR. EISEN: BIPA. BIPA simply says if you collect, use, or store information to comply with HIPAA, that is the end of the inquiry. And I think that -- I understand Plaintiffs or Plaintiff wants to bring into play various elements of HIPAA that are patient-information-focused. It can't be ignored that HIPAA fundamentally is a statute for

protecting information.

THE COURT: So, again, HIPAA doesn't protect the biometric information of the pharmacist putting his fingerprint down to open the computer system. So what you are arguing is that BIPA takes a whole swath of people, anybody who is subject to HIPAA, doctors, physicians, assistants, nurses, CNA's, social workers who work with patients, anyone who is accessing a hospital system, for instance, with a fingerprint, they are out of luck. They have no protection for their biometric information. They don't need to be told where it is being stored. They don't need to be told the retention policy. All medical providers and ancillary medical people who are subject to HIPAA are just exempt from BIPA?

MR. EISEN: I don't think that it --

THE COURT: Those who use biometric measures identifiers, I should say.

MR. EISEN: The limited subset -- and I think it is a -- this is not a wide, wholesale exemption of the health care industry; this is in a limited context of using a biometric authentication to access patient information. That is exempted under the statute because it is, I think, under the plain

language of the statute information that is collected, used, or stored for treatment, payment, or operations.

And then fundamentally, the use of a biometric authentication governing access to the health care database or to the pharmacy database in order to prescribe medication to have access to millions of patient records, that --

THE COURT: What is the purpose of this exemption?

MR. EISEN: The purpose of this exemption is to avoid any potential conflict, as I think is later detailed in the section, to avoid any potential conflict with HIPAA. And going back to what I mentioned earlier, HIPAA does require a technical safeguard. And in this instance --

THE COURT: It -- go on.

MR. EISEN: Because in this instance, the BIPA is saying if HIPAA speaks to a requirement for a health care provider, we are just not going to touch it, because the language of the exemption itself --

THE COURT: What is the purpose of the statute? You have explained that, but what was the underlying concern that was raised such that the legislature

decided this was an important exemption?

MR. EISEN: Unfortunately, there isn't a lot of legislative history to go along with this. What we have is the analogous statute in Washington state which also includes similar language, avoiding any potential conflict with HIPAA. And we have here, I think, in two different locations a clear indication from the legislature that if HIPAA requires something, we aren't going to touch it, we aren't going to -- I mean not just required, but if HIPAA speaks to this issue, this statute doesn't.

THE COURT: Well, you are saying to avoid conflict. What is the potential -- if we didn't have this exemption, what would be the conflict with HIPAA?

MR. EISEN: Well, and I should say that the language in the exemption itself doesn't speak to conflict. That shows up later on in section 25 speaking to avoiding conflict with HIPAA. But --

THE COURT: And how does this prevent a conflict with HIPAA?

MR. EISEN: This, I think, speaks more appropriately to if HIPAA speaks to a given issue, this statute does not.

THE COURT: And you are saying HIPAA speaks to this issue because it says biometric identifiers are an appropriate way to safeguard your HIPAA information.

MR. EISEN: Correct.

THE COURT: But it doesn't explicitly say that those biometric identifiers obtained by caregivers to access patient information are exempt; it says this second half of that sentence, which you believe means that, right?

MR. EISEN: Correct. The second half of this sentence, yeah, I think it is important to look at how the sentence is drafted as a whole. The first part applies to patient information. If the second half only governed the patient information, then it wouldn't have any function. It would be rendered totally moot. The statute would simply just say patient information, full stop, but it doesn't.

So the second half must mean something. The second half must mean that if information is collected to comply with HIPAA, that is covered by this exemption as well, because it doesn't say 'Patient information or patient information collected, used, or stored'; it says, "Patient

information or information collected, used, or stored."

And I don't think there is any dispute that the Plaintiffs's information was collected, used, or stored for treatment, payment, and operations under HIPAA.

The definitions of payment, treatment, and operations, which are provided under the statute itself, are very broad definitions and intentionally so. There is no way to read the definitions of treatment, payment, and operations under HIPAA without including exactly what is occurring here, and that is the use of an authentication mechanism to comply with a security rule.

Conversely, if this were not proper, then there would be a very wide swath of people -- you'd look at providers and say, 'Well, their information is covered, but the patient's, the patient's information isn't covered,' which seems anomalous. It is as if the BIPA is going to say 'Patient information or information collected, used, or stored' that it must mean more than just patient information.

THE COURT: Anything further before I turn it

over? We will come back to you for a reply as well, but go ahead if you have more.

MR. EISEN: And I just also wanted to add -- and while this is certainly ancillary -- as it relates to the claim of negligence, if the BIPA claim fails as a matter of law, the negligence claim must as well because the only duty in the negligence claim is predicated on the statutory duty. And if that duty doesn't exist, then there would be no duty here.

Likewise, there is no contention of actual damages that the Illinois Supreme Court has spoken to this clearly that potential future harm or potential emotional harm are not present actual damages. Those may be measures once actual damages have been established, but they are not in and of themselves actual damages.

And last, the additional entities named in addition to Jewel-Osco, there are certainly no allegations concerning them in any way, shape, or form.

THE COURT: Okay. Counsel?

MR. ZOURAS: Thank you, your Honor. If we start with BIPA, the statute requires the

institution of easy-to-follow, straightforward safeguards to protect biometric data, and the default rule is that all Illinois citizens are entitled to that protection.

Now, the statute includes some narrow exemptions, which, of course, the Defendant always carries the burden to plead and prove. A couple of those exemptions are all-encompassing. So, for example, there is a financial institution exemption, and that is an easy one. There there are others like the one at issue here which are conflict exemptions, the purpose of which, of course, is to avoid a conflict with other statutes, in this case HIPAA.

There is no conflict between BIPA and HIPAA here. The drafters of HIPAA wanted to ensure that there was no conflict with the patient protections already provided under that very strict statute which has very serious protections and imposes very serious penalties for their violation. So HIPAA --

THE COURT: So I am sorry to interrupt.

MR. ZOURAS: Sure.

THE COURT: But the purpose of HIPAA is to

protect patient information. Now, it involves requirements on behalf of covered entities to do that, but the ultimate purpose of HIPAA is to protect.

MR. ZOURAS: Exactly, your Honor, which would include, in fairness, biometric information of patients, so patient biometric information which is already very strictly protected under HIPAA. There are criminal penalties for the violation of HIPAA, as your Honor well knows.

So the point here is to avoid a conflict, and there is no conflict, because what the drafters did is they specifically excluded from the definition of biometric identifiers the information protected under, "under," HIPAA, and that would include things like information captured from a patient or information for health care treatment, payment, or operations, again, under HIPAA. And the statute goes on to specify some specific examples, like diagnostic tests for example.

So there is no question -- we have already established this -- the medical provider biometric data is not protected under HIPAA. There are no such protections. So the Defense is left

with trying to say that, 'Well, even though that may be the case, it doesn't matter,' because BIPA, apparently the exemption, for whatever reason -- and we have yet to identify it -- has some all-encompassing exemption for, I guess, just about anybody in the health care field that touches patient data, works with medical records, and so forth.

We keep saying, "Well, what would be the underlying purpose of this or policy, the explanation, the legislative intent?" And we have nothing but silence.

The Defendants are hung up on this "or" word in the middle of the exemption. They say it has to be disjunctive and it has to refer to two different concepts, and if we don't read that way, we have all these redundancies. What I would say, Judge, is that in this exemption, there are redundancies, there is repetition, and there is overlap.

For example, they list specific diagnostic tests, as of all of which is information captured from a patient in the first part of this. So it isn't some big crisis that there may be a

number of redundancies, repetition. They wanted it to be clear.

In many ways, it emphasizes our point that we are talking about patient data, which is the common theme. There are even internal redundancies. For example, they refer to a Roentgen process.

THE COURT: Do you mind spelling that for the court reporter.

MR. ZOURAS: I can, yes, if I'm going to have to. R-O-E-N-T-G-E-N, and I think it is pronounced "Roentgen." You know, that is another word for x-ray. There is already the word x-ray in there, and they say it twice.

So what we have here is a situation where we have a very clear exemption which is driven towards patient information, and we know that because if they wanted to exclude something else for whatever reason, provider information, mental health professional information, whatever it was, that it would have been very simple to specifically say that. The legislature doesn't draft things of that nature. They could have said, as with a financial institution, that this is an all-encompassing exemption for all, anyone who is employed or has

information taken by a covered entity.

And they wouldn't have placed it in the middle of a lengthy exemption (indicating), which is driven also entirely for patient data, and then finally we have some rational legislative purpose for it, which we have yet to hear.

The reality is that, you know, to the extent we have an "or" in there, the word "or," which Defendants are hung up on, you know, it is in the conjunctive. We know that because in its context, in the context in which it appears -- and, of course, context is driven by purpose -- this is driven towards patient information.

There is no conflict. It is very easy to comply. You can have, by the way, providers, as they did here, use biometric information. BIPA does not say don't use it. It doesn't say don't use it in the health care field. All it says is that if you are going to use it, you just have to follow some very simple and straightforward guidelines, and that is it. That is not a conflict.

And I think Defendants concede, as they have to, that it is not like there is a HIPAA mandate. There is not some specific requirement

that you use biometrics. It is one of many technical safeguard options, but it isn't --

THE COURT: And BIPA doesn't say if you use biometric safeguards to maintain the confidentiality of the records, then that biometric identifier is subject to HIPAA?

MR. ZOURAS: It does not say that. So this isn't about, you know, punishing anyone; this is about the statute says what it says. All entities that collect or maintain this data have to comply unless there is some applicable exception, exemption, whatever it might be. And that just doesn't exist here.

With respect to the two remaining arguments, we have adequately pled the negligence Count because it is based on the BIPA Count.

THE COURT: So what are the damages alleged?

MR. ZOURAS: Well, the damages are statutory, your Honor, and based on the Illinois Supreme Court's opinion in the Rosenbach case decided, I believe, in January, there does not have to be a showing of actual damages.

THE COURT: But this is not a claim under BIPA; this is a negligence action.

MR. ZOURAS: With respect to the negligence Count, Judge, I suppose that is correct.

THE COURT: "These violations have raised" -- this is Paragraph 98 -- "a material risk that Plaintiff in the putative class's biometric data will be unlawfully accessed by third parties?"

MR. ZOURAS: Yes.

THE COURT: So that seems to be a potential injury but not a realized injury at this point.

MR. ZOURAS: Admittedly, Judge, I think that's right. I do think we have some authority that an increased risk of future harm, including things like emotional harm, are recognizable, that is the Dillon case, and I cannot tell the Court at all that Rosenbach supports that. It just didn't touch upon the issue.

THE COURT: And I think counsel will probably mention this, but Williams v Manchester, I think, is the case --

MR. EISEN: Right.

THE COURT: -- that he mentioned from the Supreme Court says, well, you can plead that future risk of harm as well, but you have to have an initial injury, because this is not like a physician

left an instrument in a patient and they don't want to remove it because it will cause more harm, and so they just risk the fact that it might migrate later and so there is an injury, and then that may cause harm later.

Here, the injury is itself the failure to disclose, and the harm that may be use caused later is the potential disclosure, I guess. But I don't see how you can base a negligence claim on the fact that they didn't comply with a statute. Is there any support for that?

MR. ZOURAS: I don't, and with respect to the named Plaintiff, I cannot say that he has anything other than statutory damages, you know. I suppose, you know --

THE COURT: So it would be just a, I don't know, double recovery or it is in the alternative to BIPA, but it is reliant on BIPA?

MR. ZOURAS: I think that's right, your Honor.

THE COURT: All right.

MR. ZOURAS: And, you know, with respect to the claim that we named wrong entities because not all of them are strictly Plaintiff's employer is not an employer-driven statute. It is not that employers

have to comply; it is any entity which collects or maintains biometric data. The allegations of the complaint at this point on our motion to dismiss have to be accepted as true.

THE COURT: But you haven't alleged what these other entities' roles were in the complaints. So I think that is counsel's contention. And certainly if they were -- if, for instance, AB Acquisitions, LLC was the entity that was collecting the biometric data and retaining it, well, that would be a little closer, but at this point, I don't think there is any allegations, at least that I was able to find, that specifically identified their role in the collection retention of biometric data. Is that correct?

MR. ZOURAS: That may be correct, your Honor, at this point.

THE COURT: Okay. Anything further you want to add?

MR. ZOURAS: We would ask that the motion be denied, your Honor. Thank you.

THE COURT: All right. Counsel?

MR. EISEN: Thank you, your Honor. I think to the primary point, which is looking at the terms of

the exemption itself, to assume that the Illinois legislature intended to be redundant and worse than redundant, to use superfluous language, would run afoul of the Illinois Supreme Court's rules regarding statutory interpretation. To assume that the phrase "information collected, used, stored for health care treatment, payment, or operations under HIPAA" literally has no meaning separate and apart from the phrase that precedes it, it would be an improper read of this statute and clearly not how it is drafted.

I don't think it can be faulted that there isn't legislative history necessarily to support it, because there really isn't much legislative history, period, as it relates to this statute.

THE COURT: Well, you could see this as information captured from a patient in a health care setting such as blood, for instance, and then information collected, used, or stored for health care treatment and payment, so you would have information such as the report -- well, it guess the report wouldn't be biometric information, but you could see where the information related to the

payment for the services would be separate and apart from the actual test. So would that be a basis to conclude that it is not repetitive, it is not duplicative?

MR. EISEN: I don't know how that would be separate and apart from information collected from a patient in a health care setting in the outset.

THE COURT: Well, you get information collected from them, so it may be their fingerprint, maybe their -- well, let's say that just to have an example. And then you collect other information for payment. What biometric identifier would you collect for payment?

MR. EISEN: I -- and that is sort of, I think, our --

THE COURT: Doesn't this seem ambiguous to you?

MR. EISEN: It doesn't insofar as the definitions of -- the legislature used terms that have very specific meaning under the context of HIPAA. They use treatment, payment, and operations. Health care --

THE COURT: But they haven't qualified information, which I think is where we are at a sticking point here.

MR. EISEN: Right, because I think information, as is required under HIPAA, or I guess as it is envisioned under HIPAA, information collected, used, and stored for treatment, payment, or operations is -- it could include both patient information, it could include provider information as well, because that information is instrumental particularly to treatment and operations. If -- I mean, it --

THE COURT: And that second portion of the sentence, it could be read as any information as collected pursuant to HIPAA, right? And then you are saying that because HIPAA allows you to use biometrics, the biometric information of the pharmacist is collected pursuant to HIPAA.

MR. EISEN: Correct.

THE COURT: So I don't see that last connection. I mean, it is collected because it is one of the options HIPAA gave them, but HIPAA didn't require that it knew that and doesn't separately mention or discuss the protection of the pharmacist's fingerprint, for instance.

MR. EISEN: So what HIPAA does speak to are the duties and the operations of the covered entities.

THE COURT: To protect patient information.

MR. EISEN: Correct, to protect it.

THE COURT: Not to protect caregivers' information.

MR. EISEN: But I might add if the covered entity does not adequately protect it, if, for example, the fingerprint mechanism, the biometric authentication mechanism was implemented improperly or didn't work, HIPAA would punish that covered entity for improperly protecting the patient information.

So while, yes, it may not speak exactly to information collected from a treating physician, and in our opinion it would be, I think, odd to read the statute such that if a -- you know, you can envision an emergency room physician accessing the computer to pull up a client file, and if that physician or if that doctor hasn't signed the word-for-word BIPA consent authorization document, so there isn't a publicly available retention policy, that physician can then turn around and sue even though in the emergency situation, it would be a little bit odd to force that physician to sign off before using the database or to punish the entity for not having a publicly available retention

schedule before using the database.

This system protects millions of patient records throughout the country. And to put Albertson's in a position where they are facing a minimum of $1,000 per pharmacist, and Plaintiff hasn't yet articulated what they believe a measure of damages would be, but $1,000 per pharmacist simply because they were trying to implement a technical safeguard that HIPAA requires them to implement, it doesn't necessarily speak to it must be biometric; it leaves up to the health care provider, pick the best one that works in your scenario.

It doesn't say biometric versus password, and it is in light of recent data breaches, passwords simply aren't the best means to protect. So a biometric authentication was implemented. To put Albertson's in a position where there are looking at $1,000 minimum per pharmacist, because Plaintiff's counsel is saying there wasn't a publicly available retention schedule, even though this particular pharmacist claims he participated in implementing this very system, seems bizarre.

And I don't think it fair to Albertson's

to read this language which clearly relates to information collected, used, or stored for treatment, payment, or operations. This information was collected, used, and stored for treatment, payment, and operations. I don't think there is any way to read HIPAA and the definitions of treatment, payment, or operations, without encompassing what the covered entity is doing.

The term particularly health care operations is a very broad term speaking to what the covered entity must do to facilitate treatment and payment. This was accessed in order to prescribe medication. This is not, I think, what the legislature had in mind with people losing control of their biometric information or a company going bankrupt and their records are everywhere now.

THE COURT: Well, and to your point, HIPAA's definition of health care operations includes business management and general administrative activities of the entity.

MR. EISEN: Correct.

THE COURT: So it wouldn't just include accessing a medical record.

MR. EISEN: Correct, but it would include

accessing it. And --

THE COURT: Correct.

MR. EISEN: And by that point, yes, the computer, the health care -- the pharmacy computer can be used to do other things once an authorized person has accessed that computer.

And the health care field is heavily regulated. HIPAA requires technical safeguards that Albertson's chose to implement a biometric authorization mechanism. It clearly falls within the guidance of this language, and to read that latter phrase is doing no more than modifying the former phrase, it will result in extraordinary liability across the health care sector under this statute, because it is very common, I would say more common than not, for it to use biometric authentication measures in hospitals, in doctors' offices, and in pharmacies.

THE COURT: And you are meaning all of these health care providers without any protection of their privacy because they are not protected under HIPAA and they are not protected under BIPA?

MR. EISEN: They are protected insofar as these mechanisms must be implemented and effectively so,

if the biometric authentication mechanism isn't effectively implemented.

THE COURT: But you are saying they can't sue -- their fingerprint is taken, but they can't sue to ensure that whoever is requiring them to comply didn't properly disclose and what not.

MR. EISEN: And I don't think that that is what --

THE COURT: But they are not protected under HIPAA either. So they are in this doughnut hole, and you think that is what the legislature intended when they put this exclusion in and when they wanted to have BIPA not conflict with HIPAA is to leave all these people in this doughnut hole where they have no protection for their biometric identifiers? I think that is what you are saying.

MR. EISEN: But frankly I do, because neither the patients -- patients can't sue under HIPAA. The health care employer might be punished, but patients can't do it. If the health care provider wanted to take biometric records and throw them in the middle of the street, patients couldn't do anything about it.

THE COURT: But there is a reason for this in

that if you specifically if you have an emergency and you are going to be taking blood, you don't want to have to require a consent before you take the blood. That is a recognized purpose that I think everybody can get on board with. You don't want to have to stop health care in order to get a consent.

I mean, most hospitals give consents to anyone who comes into the hospital and they are awake and they are cognizant, but there are so many situations where that is not the case and they can't get that done, and that would result in a violation of BIPA. So counsel has put forth that is why this exemption was in place.

But if we go by your interpretation, then any physician or nurse or social worker who uses his or her fingerprint to access any records or for the operation of the hospital cannot then sue anybody if it hasn't been disclosed to that person, can't sue if there is no retention policy that has been provided to that person, can't protect their privacy.

MR. EISEN: So I think it is important to point out that I think a very easily articulable purpose in having this section of the statute apply to

providers is that if a pharmacist, if a doctor were to say, 'No, I'm not signing that,' then the hospital now has to have two different forms of identification: One for those who did agree, and one for those who didn't. And that, I think, is going to create a lot of costs in the health care industry if you have two different measures of authentication to implement to adhere to --

THE COURT: I am not following that argument. Can you explain it in more detail?

MR. EISEN: So the consents required under BIPA to use a biometric authentication, which again we submit, should this case proceed, that hasn't been accomplished here. Plaintiff didn't agree to that consent. But if a pharmacist were to say no or if a doctor were to say, 'No, I am not going to sign that, I am not going to give you authorization,' then either the health care provider would have to fire the doctor or would have to implement some other means of authentication only for that doctor.

THE COURT: And how does that apply to this case?

MR. EISEN: Because what this section is intended to do is say, 'If HIPAA speaks to it, we're

not going to touch it,' because if BIPA does speak to this information, then what BIPA would effectively do is require two different means of authentication, would require a hospital or a pharmacy, say, 'You can use biometric authentication for those who agree to it, and you must use some other method for those who do not.' And that, I think, is in conflict.

THE COURT: So that cannot have been the intent of the legislature? Is that what you are saying?

MR. EISEN: Correct. I think the legislature's intent here is to say, 'If HIPAA speaks to this issue, we aren't going to touch it.'

THE COURT: Okay. But in the alternative, I think we have all talked about this five times, HIPAA doesn't speak to the protection of the privacy of the physicians' biometric information, the fingerprint.

MR. EISEN: That is --

THE COURT: And you said if HIPAA speaks to it, we are not going to touch it. So here you are saying BIPA says we are not going to touch it, but HIPAA is not touching it either.

MR. EISEN: HIPAA does speak to it to the

extent that it requires a technical safeguard.

THE COURT: Right, but it doesn't protect that information. It requires a technical safeguard to protect patient information, but it doesn't protect the technical safeguard information, unless I am missing something in HIPAA. But you see what I mean? There is the doughnut hole, I think.

MR. EISEN: I see what you mean, but I don't think that that is an unintended result. I think what the legislature is saying if, for example here, because HIPAA -- I don't think that the legislature could have intended a myopic view of HIPAA as, 'We are only going to talk to -- this exemption will only concern protected health information,' because they could have just said it.

They could have just said, 'Patient information or protected health information is defined under HIPAA.' That would have been very easy. That would have avoided, I think, this motion in its entirety, but it didn't, and instead it chose three words which have very clear meaning and apply almost entirely to only things covered entities do. So I think to --

THE COURT: But you are still not getting to

how would the legislature -- the legislature didn't care then? It said, 'Physicians are not protected, and it sucks for them, but we are not going to do it'? I mean, I understand your arguments, but I still come back to the fact that this leaves them out.

And if they were going to leave out medical providers covered, you know, that are required to comply with HIPAA, you would think that they would put that out there and put it directly in.

MR. EISEN: But I don't think that a broad-based exemption is what the legislature had -- because there are certainly circumstances and we have seen enough biometric lawsuits over biometric time clocks or clocking in and out of work, hourly employees. And would those employees be covered here? I don't think that exemption would cover them.

But here we are talking about accessing a pharmacy database, so I think the legislature could say, 'Look, we are not going to try to get into the nitty-gritty of what type of person in the health care field, if the pharmacy janitors are covered or

not; what we are going to do is use these terms as defined under HIPAA.'

And to be fair, there are fairly wide groups of people that aren't covered. There is a biometric time clock in the hallway of this courthouse because state employees aren't covered. And there are a whole swath of state employees that simply are not covered.

But here, rather than do that, I think the legislature said, 'Well, we aren't going to get into who is and who isn't because there are circumstances of which it would not be appropriate.' But here, if it falls within these three definitions, that means the plain language of the statute.

THE COURT: And then I am reading anyone within the hospital, for instance, who is involved in billing, even repairs, custodial staff, anybody then, because operations, this includes customer service, it includes payment, of course -- I'm sorry. Payment is separate, then operations, it includes general administrative activities. I guess that would include custodial possibly. But you are talking about anyone employed by the hospital that

is involved with billing or administrative activities?

MR. EISEN: I don't think that is necessarily true. I don't know that if there are --

THE COURT: Then --

MR. EISEN: Sorry, if they are an hourly employee if a time clock to clock in and out of work is covered, but if they have access --

THE COURT: Well, I am just saying if they have to use their fingerprint to access the medical record to start the payment process --

MR. EISEN: Right.

THE COURT: -- or if they have to access the medical record to address an administrative complaint under operations.

MR. EISEN: I think that would be covered. Again, I don't think we need to go --

THE COURT: That would be an exemption.

MR. EISEN: Right. I don't think we need to go any further than the language the legislature used, which was collected, used, or stored for health care, treatment, or operations under HIPAA. And I don't think that could be reasonably disputed that data is collected, used, or stored for health care,

treatment, or operations.

Moreover, wouldn't we as patients want the best protection? I don't think that is unreasonable to say -- you know, if my physician has a biometric authentication, I would be happy about it. I want to make sure that they have best --

THE COURT: But you wouldn't care that their information is not -- you can't protect it?

MR. EISEN: I --

THE COURT: Because that is what you are saying here. It's like, 'I'm glad they have it for my patient's safety of my records, but too bad that they can't protect their own privacy.'

MR. EISEN: To a certain extent, I suppose that's true. But I think it is also important to know that BIPA doesn't really have security protections. So we are not really talking about a statute intended to protect physician information.

THE COURT: So it is a disclosure statute.

MR. EISEN: It is a disclosure statute, period.

THE COURT: But there is a way for someone to stand up and say, 'Yes, you are requiring that I do this, but you then need to follow this, which tells me that it is being protected.'

Because if you retain and you store properly and then if you have a retention schedule and if you have those procedures in place, are these the best to protect the biometric information.

MR. EISEN: Right.

THE COURT: So there is an enforcement to confirm the enforcement mechanism and the disclosure mechanism is to say, 'Hey, we are doing all this,' and then the enforcement mechanism is saying, 'Well, you are not doing this, so it is not protecting my information.'

MR. EISEN: I mean, I think to the extent HIPAA has strict security options, BIPA simply doesn't; it is just says protect it like you would protect anything else, which in this context would, you know, protect it as you protect patient information.

But the plain language of the statute, I do believe, speaks to this issue. And to read pharmacists' information out of the language of that statute would be to give that statute, to read that later phrase as having virtually no meaning, I mean, it is difficult to think of a scenario, as we are trying to, where patient information could be covered by Section 1 or not covered by Section 1 but

covered by Section 2.

It's very -- it would be -- jumping through, I think, linguistic hurdles to try to find a scenario where that would occur, and I realize we spent a good deal of time talking about what might happen or if physicians' information, pharmacists' information isn't protected under HIPAA, there would be a wide group of people not protected under HIPAA.

But the statute says what it says, and reading the statute to speak only to patient information, I think we would have expected the legislature to say either captured from a patient in the health care setting or patient information collected, used, or stored, or would just have said protected health information under HIPAA, period, but it didn't.

And reading pharmacists' information out of this statute, out of this language, would eliminate the second half of that phrase entirely from the statute, because again it is difficult to envision what wouldn't fall under Section 1 but fall under Section 2.

And I do think as a -- and I hesitate to make a policy argument, but in this circumstance, if

a pharmacy like CVS, if this exemption doesn't apply, then we will, I think, be left with a scenario where all health care providers will need to implement alternative means of complying with the technical safeguard, because if physicians or pharmacists --

THE COURT: No, they would just have to comply with BIPA.

MR. EISEN: But if a pharmacist says, 'No, I am not signing that,' then they do need to implement something in order to have that --

THE COURT: Well, okay.

MR. EISEN: And that is not something, I think, HIPAA -- that HIPAA would require a pharmacy to implement alternative measures if they think one is the best.

THE COURT: No, but if there are going to take the fingerprints, BIPA requires that they follow certain measures. They choose another option or have to do another option because someone opts out, they can do another option that is not subject to BIPA.

MR. EISEN: Right, but what they would end up doing is they would be implementing a measure that

the health care provider believes isn't as good.

THE COURT: What if that happens under another scenario. I know it is not subject to HIPAA, but you have an employer, and you have somebody say, 'I want to work here, and I'm working here, and I don't want to use my fingerprint.' They would have to do the same thing. If they didn't just fire the person, they would have to come up with an alternative system to clock them in and out.

MR. EISEN: Right. There is no required -- I mean it is not required under HIPAA, but what I think makes it unique is that it requires health care providers to use what they believe is the best method to protect patient information.

THE COURT: But it is not required to use fingerprints biometrics.

MR. EISEN: Correct.

THE COURT: That is one option.

MR. EISEN: But if a health care provider were to say, 'That is the best, but I can't use it here,' they would have to use an option that they deem second best, which would possibly expose them to liability because they are using a means of protecting patient information that they believe

isn't as secure.

THE COURT: Okay. I am just going to take a few minutes' recess, and then I will return to rule. Thank you.

MR. ZOURAS: Thank you, your Honor.

(Whereupon, a recess was taken.)

THE COURT: Okay. As I mentioned before, we are here on Defendants' 619.1 motion to dismiss. I have reviewed the briefs, the motion, as well as heard oral argument today, and I am ready to rule.

We will start with the easier rulings first, which is with respect to the negligence Count and the dismissal of the entities besides New Albertson's Inc., d/b/a Jewel-Osco. I am going to grant the motion to dismiss related to those two arguments. The negligence Count will be dismissed. There is no actual damages that have been alleged such that counsel could argue future damages may arise.

With respect to the other entities that are named, there are no allegations in the complaint addressing their involvement in the disclosure, the use, collection, retention of the biometric information, and therefore there is no indication

that they were involved in these activities, so there would need to be some connection. So those are both dismissed.

The parties in the negligence claim are dismissed without prejudice, but there would need to be a showing as to actual damages to alleged negligence, as well as there would need to be a showing that these parties had direct involvement with the requirement to provide biometric information, the collection of that information, the retention of the information, those types of things.

So then on to the first argument. Both sides argued that the exception in BIPA, which is 740 ILCS 14-4/10 is unambiguous. Both parties have argued what they believe are plausible readings. And in looking at the statute itself, without looking at anything else or considering anything else, they are both plausible readings, and therefore because of that, the statute is ambiguous, which is when the court would look to legislative history.

And no legislative history has been presented to the court, and it sounds like there is little out there. With that, then the court must

look to the intent of the statute. And I should also note there are no other cases on point. This is an issue of first impression.

To read the exception as Defendants set forth is nonsensical, in this court's opinion, essentially that Defendants argue a blanket exemption for doctors, nurses, physical therapists, CNA's, ultrasound technicians, anyone subject to HIPAA who uses biometric information to access medical records or billing records or hospital records. These large categories of workers cannot look to BIPA to protect their privacy. If the General Assembly intended to exempt BIPA for anyone subject to HIPAA, the legislature would have said so. That should have been set forth, would have been set forth more clearly.

Counsel for Defendants stated that if HIPAA speaks to it, then BIPA is not going to touch it. Well, HIPAA does not protect the privacy of caregivers' biometric information. So it is, again, in a doughnut hole, which is not what I believe the legislature intended.

Counsel mentioned that it is statutory construction, we can't look to a statute and read in

redundancies, which is true; however, the statute, if you look to the other definitions, has some very clear redundancies, especially with respect to private entity, which I guess I will just read into the record for clarity.

This is, again, 14-4/10: "'Private entity,'" quote/unquote, "means individual partnership, corporation, limited liability company, association, or other group however organized. A private entity does not include a state or local government agency. A private entity does not include any court of Illinois, a clerk of court, or a judge or justice thereof."

There are redundancies in that definition. Understanding that we are not to read redundancies in, but it is clear that there are additional redundancies in other definitions, a point to make.

And, again, under Defendants' reading, BIPA would provide a private right of action for everyone except for health care providers to protect their biometric information. Again, that is a doughnut hole that I can't fathom that the legislature intended.

And reading BIPA to cover pharmacists in this case is not in conflict with HIPAA. BIPA is a disclosure statute with respect to biometric information, and HIPAA protects patient information.

Finally, Rosenbach, obviously not directly on point to the issues here, but Rosenbach did point out, the Supreme Court pointed out, that biometric privacy is important and that protection should be broadly applied. To interpret the exclusion to include all HIPAA providers does not comport with Rosenbach's broader application.

So the motion to dismiss based upon the exception is going to be denied. That's it.

MR. ZOURAS: Your Honor, do you want to set a time frame for an answer and a follow-up status on any one of those points?

MR. EISEN: Yes, and that would depend in large part on what you want to do as it relates to the negligence and the other entities. If things are going to stay as they are, then I suppose that there is going to be an amended complaint. I assume we should figure days out of that.

MR. ZOURAS: Sure. So we will stand upon our current complaint in light of the court's order. So

with that, we can set time frame.

THE COURT: Okay. 28 days?

MR. EISEN: That would be one way out of this at the time, especially in light of the holiday, if you want to do that.

THE COURT: Sure. If you want 35, I can give you that.

MR. EISEN: Sure. Why not. We will take it.

THE COURT: That is to be 35, and then we will come back maybe in 60 days, assuming it is going to be an answer. That way typically if I find out there is going to be a motion, I will bring you back earlier so we can set a briefing schedule. So why don't we just do a 60-day status date.

MR. EISEN: Sounds good.

(Which were all proceedings had in the above-entitled cause on this date.)

STATE OF ILLINOIS)
) SS:
COUNTY OF C O O K)

I, ANDREW ROBERT PITTS, C.S.R., a Certified Shorthand Reporter within and for the County of Cook and State of Illinois, do hereby certify that I reported in shorthand the proceedings had at the taking of said hearing and that the foregoing is a true, complete, and correct transcript of my shorthand notes so taken as aforesaid and contains all the proceedings given at said hearing.

IN WITNESS WHEREOF, I do hereunto set my hand and affix my seal of office at Chicago, Illinois this 8th day of July, 2019.

_____

Certified Shorthand Reporter
Cook County, Illinois
My commission expires May 31, 2021

C.S.R. Certificate No. 84-4575.