

Andrea Lynn Chasteen
Will County Circuit Clerk
Twelfth Judicial Circuit Court
Electronically Filed
18CH1327
Filed Date: 7/8/2019 4:49 PM
Envelope: 5682834
Clerk: KA

Exhibit 1

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

1 APPEARANCES:

2 STEPHAN ZOURAS, LLP, by
3 MR. JAMES B. ZOURAS
4 MR. ANDREW C. FIZCKO
5 205 North Michigan Avenue
6 Suite 2560
7 Chicago, Illinois 60601
8 312.233.1550
9 jzouras@stephanzouras.com
10 afizcko@@stephanzouras.com

11 Appeared on behalf of the
12 Plaintiffs;

13 BENESCH, FRIEDLANDER,
14 COPLAN & ARONOFF LLP, by
15 MR. MARK S. EISEN
16 333 West Wacker Drive
17 Suite 1900
18 Chicago, Illinois 60606
19 312.212.4949
20 meisen@beneschlaw.com

21 Appeared on behalf of the
22 Defendants.

23
24

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

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

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

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

10 MR. FICZKO: Good morning, your Honor. Andy
11 Ficzko on behalf of Plaintiff.

12 THE COURT: Okay.

13 MR. EISEN: Mark Eisen on behalf of Defendants.

14 THE COURT: All right. This is Defendants'
15 2-619.1 combined motion to dismiss. If you would
16 like to begin.

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

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

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

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

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

19 MR. EISEN: I'm sorry.

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

22 MR. EISEN: HIPAA speaks to --

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

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

5 THE COURT: How so?

6 MR. EISEN: HIPAA speaks to protecting patient
7 information.

8 THE COURT: Patient.

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

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

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

21 THE COURT: I am not saying that it did.

22 MR. EISEN: Sure.

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

24 MR. EISEN: Right. And I appreciate that point

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

8 THE COURT: I'm sorry?

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

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

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

1 those definitions which we recited in our reply.

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

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

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

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

1 under HIPAA but not BIPA?

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

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

5 MR. EISEN: Correct.

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

8 MR. EISEN: Correct.

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

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

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

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

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

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

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

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

24 THE COURT: Patient information, yes, but we

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

8 MR. EISEN: Right.

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

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

13 THE COURT: If you are arguing it does.

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

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

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

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

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

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

18 MR. EISEN: Correct.

19 THE COURT: Correct? Okay.

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

1 patient information.

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

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

16 THE COURT: From the patient?

17 MR. EISEN: From the physician.

18 THE COURT: For his fingerprint, for instance?

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

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

1 his biometric information specifically.

2 MR. EISEN: Right, but it --

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

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

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

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

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

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

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

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

24 THE COURT: How are they punished for the

1 safeguard that they choose in that scenario?

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

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

17 THE COURT: Which statute?

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

1 protecting information.

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

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

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

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

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

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

9 THE COURT: What is the purpose of this
10 exemption?

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

17 THE COURT: It -- go on.

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

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

1 decided this was an important exemption?

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

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

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

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

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

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

5 MR. EISEN: Correct.

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

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

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

1 information or information collected, used, or
2 stored."

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

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

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

24 THE COURT: Anything further before I turn it

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

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

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

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

22 THE COURT: Okay. Counsel?

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

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

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

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

22 THE COURT: So I am sorry to interrupt.

23 MR. ZOURAS: Sure.

24 THE COURT: But the purpose of HIPAA is to

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

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

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

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

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

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

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

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

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

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

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

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

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

1 information taken by a covered entity.

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

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

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

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

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

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

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

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

17 THE COURT: So what are the damages alleged?

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

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

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

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

7 MR. ZOURAS: Yes.

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

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

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

20 MR. EISEN: Right.

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

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

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

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

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

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

20 THE COURT: All right.

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

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

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

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

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

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

22 THE COURT: All right. Counsel?

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

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

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

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

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

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

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

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

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

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

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

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

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

15 MR. EISEN: Correct.

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

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

24 THE COURT: To protect patient information.

1 MR. EISEN: Correct, to protect it.

2 THE COURT: Not to protect caregivers'
3 information.

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

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

1 schedule before using the database.

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

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

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

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

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

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

21 MR. EISEN: Correct.

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

24 MR. EISEN: Correct, but it would include

1 accessing it. And --

2 THE COURT: Correct.

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

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

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

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

1 if the biometric authentication mechanism isn't
2 effectively implemented.

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

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

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

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

24 THE COURT: But there is a reason for this in

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

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

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

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

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

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

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

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

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

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

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

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

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

19 MR. EISEN: That is --

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

24 MR. EISEN: HIPAA does speak to it to the

1 extent that it requires a technical safeguard.

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

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

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

24 THE COURT: But you are still not getting to

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

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

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

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

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

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

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

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

1 is involved with billing or administrative
2 activities?

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

5 THE COURT: Then --

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

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

12 MR. EISEN: Right.

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

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

18 THE COURT: That would be an exemption.

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

1 treatment, or operations.

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

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

9 MR. EISEN: I --

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

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

19 THE COURT: So it is a disclosure statute.

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

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

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

5 MR. EISEN: Right.

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

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

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

1 covered by Section 2.

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

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

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

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

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

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

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

12 THE COURT: Well, okay.

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

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

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

1 the health care provider believes isn't as good.

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

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

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

17 MR. EISEN: Correct.

18 THE COURT: That is one option.

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

1 isn't as secure.

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

5 MR. ZOURAS: Thank you, your Honor.

6 (Whereupon, a recess was taken.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 with that, we can set time frame.

2 THE COURT: Okay. 28 days?

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

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

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

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

15 MR. EISEN: Sounds good.

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

19

20

21

22

23

24

1 STATE OF ILLINOIS)

2) SS:

3 COUNTY OF C O O K)

4

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

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

16

17

18

19 _____
Certified Shorthand Reporter

20 Cook County, Illinois

21 My commission expires May 31, 2021

22

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

24