II. USE OF PATIENT INFORMATION IN ARBITRATION OF HEALTH CARE EMPLOYEE DISCIPLINE: SUBSTANTIVE AND PROCEDURAL ISSUES

While arbitrators generally prefer to resolve cases based on the "law of the shop" rather than external law and policy, consideration of external law and public policy may be unavoidable when contractual "just cause" disputes in the health care industry implicate rules and laws designed to protect privacy of patient medical information, including, in the United States, the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[54] An employer or union may assert a need to use medical information about a patient to defend or challenge the employer's discipline of a health care worker. Employers may seek to discipline or discharge employees for violating patient privacy laws or policies. Patient medical privacy issues may arise as questions of procedure, such as the disclosure or admission of evidence, or they may arise as questions of substance, such as which violations of employer privacy rules should subject an employee to discipline and, when appropriate, whether the measure of discipline should vary depending on the nature of the violation. In this session, experienced advocates who represent health care workers and employers briefly argued their positions on a series of challenging scenarios, and a distinguished labor arbitrator explained her reasoning process in resolving these disputes.

Moderator: **Laura J. Cooper,** National Academy of Arbitrators, Minneapolis, MN

Panelists: **Arbitrator: Patricia Thomas Bittel,** National Academy of Arbitrators**,** Cleveland, OH
Union: Brendan Cummins, Miller O'Brien Cummins, Minneapolis, MN
Employer: Timothy Kohls, Allina Hospitals & Clinics, Minneapolis, MN

Laura Cooper: The topic that brings us here this afternoon is a complicated one. There is a vast body of federal law and regulation, as well as state law, that governs the privacy of patient records. And those laws are committed to the proposition that maximum

[54]Pub. L. No. 104-191, 110 Stat. 1936 (1996).

protection should be given to patient records. But our question is: What happens when those very same records are critical to a party's proof in a discipline or a discharge case? The records may be critical to the health care provider's or the union's case, or both. Is there some way to accommodate the interest in a fair and full record while also respecting the patient's privacy rights under the law? We're going to talk through a series of scenarios.

Scenario A

Laura Cooper: A patient was wheeled down a corridor by a nursing assistant and thereafter complained of being mishandled by the nursing assistant. As a result, the nursing assistant receives a five-day suspension that the union grieves. What's at issue here is a video. There's a camera in the corridor that has recorded these events and, two weeks before the hearing, the union asks the employer for a copy of the video. The employer refuses, saying two things, "The patient does not grant permission for its release and, besides, we don't want the union workers to know where these cameras are that are monitoring the corridors."

I'm going to ask Mr. Cummins to make a brief argument on behalf of the union.

Brendan Cummins: Starting with the security camera location, I would argue that the employer doesn't have a significant confidentiality interest in the location of the camera. Any purported confidentiality interest is greatly outweighed by the necessity of the video showing what exactly happened in the incident in question. I would also note that the National Labor Relations Board (NLRB) has held that the placement of cameras in the workplace and whether or not they're secret is a proper subject of bargaining. If it's a proper subject of bargaining, then it's not an absolute management right, and the location could be compelled in an arbitration.

As to the video and the patient confidentiality interest, I would request a subpoena and note that the HIPAA regulations permit disclosure of the video as long as there's a qualified protective order in place. So I would propose a qualified protective order that would limit the use of the video to the arbitration proceeding and provide for disposition of the video after the proceeding either by its destruction or return to the hospital.

Laura Cooper: Mr. Kohls, what is the employer's perspective on this issue?

Timothy Kohls: I will start with the patient's authorization issue first, mainly because I like the argument a little better. In this context, I would say we're not permitted to disclose under the facts that we have. Right now, it's just a request from the union for a copy of the video. We are not permitted under HIPAA to disclose it at this stage. Even if there was a subpoena issued, as Brendan pointed out, that's not an absolute right to have it. It does have to be accompanied by either notice to the patient, and that would have to come from the party requesting the information, or a qualified protective order. And if Brendan were on the other side of the case with me, we would probably spend some time talking about what that protective order would look like.

In regard to the hidden camera, I guess I would take the exact opposite position, saying we absolutely do have a legitimate interest in maintaining the confidentiality of the location. It's necessary for the maintenance of our operation, and there's no evidence in this case that we haven't bargained the ability to use secret cameras. I don't think then we'd be obligated to disclose the locations, just in this case.

Laura Cooper: Ms. Bittel, as the arbitrator, how would you rule in this case and what further information would you need?

Patricia Bittel: I'm going to complicate things a little bit. But first of all, as to the location, there's no contractual right to protect the confidential location of the camera. Management can move it any time to any place they want to. So I don't see much damage to them by the location being revealed. I'm not too concerned about the location argument.

The patient's refusal to authorize use of this video gives me great pause; there's a red flag. All antennas are up because now we've got a potential liability if we use it improperly or when it's not been properly authorized.

Now, on that subject, I attended Briar Andresen's presentation yesterday.[55] Her opinion was that all health care organizations should require arbitrators to sign a document known as a business associate agreement. It may have a lot of obligations in it that would make me and maybe you very uncomfortable. For example, my office is attached to my home, and I do not lock my filing cabinets when they are not in use; I don't even know if I have the key to them. If there's going to be a recommendation published that

[55]See Part I of this chapter, "HIPAA Basics for Arbitrators."

we start being asked to sign these agreements, we need to look at them. We need to start thinking about this.

I personally would be disinclined to sign such an agreement, which would lead me to the following: If the parties will stipulate to a qualified protective order, that helps a lot. If I had a subpoena with a stipulated, qualified protective order, I'm more comfortable now. I certainly can issue a qualified protective order on my own. But in this particular case, where there's a patient who says, "No, I don't want you to use that," there are two options: One is to de-identify the video, and the other one is to say, "Brendan, you've got to go to court, and here's the subpoena, but you've got to enforce that in court," because the statute limits subpoena power to a court, an administrative tribunal. So, I'm not comfortable.

Timothy Kohls: Yes, to one of Patti's points. In the HIPAA regulations, the protective order has to be issued by either a court or an administrative tribunal. Although the term "administrative tribunal" is not defined anywhere in the regulations, it seems the best reading of it is that it would be a government agency, not a private arbitrator.

Brendan Cummins: I would take issue with that just slightly. The HIPAA regulations do allow for disclosure pursuant to court order or order of an administrative tribunal, but also in response to a subpoena discovery request or other lawful process that is not accompanied by an order of a court or administrative tribunal if there's a qualified protective order in place.

Timothy Kohls: Yes, but there in the regulations it says that the qualified protective order must be an order of the court or an administrative tribunal. So I think the protective order would have to come from a court, not from the arbitrator.

Laura Cooper: I think in this regard it's the health care entity that has the legal obligation to protect the information, not the arbitrator, unless the arbitrator is under one of these business associate agreements. So from the perspective of the arbitrator and what he or she might confront at the hospital, saying "I'm not going to reveal it until I have a court order," as Ms. Bittel says, then it's the obligation of the party that seeks to obtain the information to get the court order.

The other thing I wanted to note is that our conversation has dealt with the federal law, the HIPAA provision. But in most states there are also laws with regard to the privacy of patient records, and those are different. Under the federal law, the state law is preemptive if it is more protective of patient privacy. So for most of us

who practice in multiple states, it may be very tricky to be advised of health care privacy laws in a variety of states.

Ms. Bittel, you had a suggestion of how arbitrators might deal with that going forward.

Patricia Bittel: I tend to think in practical terms. This is a very esoteric subject. But my practical suggestion is, if you have a case where one of the parties is a health care provider, then you might want to set up a pre-hearing conference call to see if there are going to be any of these issues, to see if you're going to be confronted with a decision about whether or not to tell a party that they've got to get a court order, to see if somebody's going to ask you to sign something. Just to get everything out on the table well before the hearing, because there's a lot that can happen. You don't want to wait until the day of hearing and then have to postpone and have another hearing. These are foreseeable issues that can arise.

The other thing we need to go into a little bit further on this scenario is the difference between redaction and de-identification, because, as arbitrators, a lot of us live in the comfortable world, which is a false security, that if you've redacted the document or you've blotted out the face of the patient, then you're fine. Nobody can tell who it is, and so there's no possible liability. In point of fact, that's not true; de-identification has specific statutory criteria that are incredibly stringent. For example, if you completely blotted out the face of this patient but the video is tagged with a date, it's not de-identified. It's still private health information.

Laura Cooper: If a document or a photograph has any single one of the identifying pieces of information on it as presented in Part I, then it's still HIPAA-protected information and then would need the protective orders and court orders or patient permission as we have discussed.

Scenario B

Laura Cooper: A hospital has a typical policy prohibiting employees from taking any photographs within the hospital or of any patient without permission. But in that policy, there's an exception that says photographs may be used for staff training if the patient's identity is not revealed. A registered nurse is caring for a patient who has a particular kind of arm injury that makes it tricky to insert an intravenous line. She figures out a way to do

it. In the hope of instructing other nurses in that technique, she goes to her locker, gets her cell phone, and takes a photograph of the patient, taking care to make sure that the patient's face is not revealed. She is, however, disciplined for violating the rule about taking photographs of a patient. The hospital maintains that it's only official staff training purposes for which photographs of patients may be taken, even those in which a patient cannot be identified.

Subsequent to the nurse's discipline, the hospital has a training session on HIPAA issues, as it does periodically. At that training session the hospital is very careful to instruct the nurses that when the rule says "photographs may be used for staff training purposes only," that means official staff training purposes and not individual employee initiatives for training purposes. The union now wishes to offer evidence of that subsequent staff training and the hospital objects on the grounds that the information is a subsequent remedial measure.

You want to start, Tim?

Timothy Kohls: The training is a subsequent remedial measure and not relevant to the inquiry. The inquiry here is really about what the employee knew prior to taking the photograph with her cell phone and not what happened subsequently. Under those grounds, the rule of evidence would clearly exclude it.

I expect my friend, Mr. Cummins, to say that it is relevant. It would be asserted that the prior training on the rule was somehow inadequate. I'd take issue with that. It's common for employers to routinely update their training to use real-life examples. I think that we want that—it's good practice for employers to have their training evolve with the world. Just because employers are getting smarter, it doesn't mean that they were foolish before. It's a subsequent remedial measure and should be excluded.

Also there's a little bit of policy in this one that is applicable. The policy underlying the subsequent remedial measure is that parties take steps to make sure that whatever happened doesn't happen again. In this instance, we're talking about protected health information and ways to make sure that remains confidential. There's some merit to the argument that we should enforce that policy so that employers don't feel stifled in their subsequent training, to make sure their training can evolve with the evolving role.

Laura Cooper: Mr. Cummins?

Brendan Cummins: I would argue that the subsequent HIPAA training is admissible and indeed highly probative, because it

tends to show that this policy of requiring supervisory approval or that the photos be part of official hospital training materials was not clearly communicated at the time of the incident in question. In fact, it may have been adopted after the fact. Mr. Kohls mentioned the importance of the policy of HIPAA confidentiality.

There's another policy at stake here, and that's just cause. A crucial element of just cause is that the employee has advance notice of the probable consequences of her conduct. This subsequent training indicates that the employer didn't make the message clear in advance that supervisory approval was required. Therefore, it really goes directly to the heart of just cause, and the evidence should be admitted.

Laura Cooper: Madam Arbitrator, how would you rule?

Patricia Bittel: I would let the evidence in, because this is the last step of the grievance procedure. If the union were holding on to something that it felt was critically important to the case, then I want them to have an opportunity to go ahead and get that out so that they can feel that they've been heard. At the end of the day, I am sensitive to the public policy issue. I also don't think that this evidence is particularly helpful because this case revolves around a notice issue, notice of the rule. The employee, regardless of what happened at the later time she acted, did not have clear notice of this rule.

I would never say this to you at hearing, Tim, but why would you discipline this employee? Here you've got someone who's coming up with a new and better way of doing things and you're slapping her hand. This is the kind of employee you should counsel, or at the most give a letter of reprimand. It doesn't say what kind of discipline she received, but I would not be in favor of particularly heavy discipline. Certainly she should have known that, when training is occurring, management would have some concern about how that's done and what that would be.

The use of her cell phone is a factor and evidence of distribution of the photograph or loss of control of the phone would be troubling. But there is no such evidence. In my mind, this can be seen as a very mild offense. She should be counseled.

Laura Cooper: Hospitals are really concerned about cameras, as are nursing homes and the like. It used to be that people didn't bring cameras to work, so it wasn't so much of an issue. Now, pretty much every employee has a camera in a pocket or a handbag or a locker, and they're much more freely available.

The other thing I should note is that this particular photograph is potentially not HIPAA-protected. If the patient's face is not visible and if there's no date on it, then it satisfies the criteria for de-identified material. But, of course, that doesn't mean it might not be a violation of employer policy. Employers are free to have—and indeed do have—stricter policies than the law requires, and they are entitled to enforce them so long as the notice is clear.

Patricia Bittel: As to the employee who did this, I would be curious to know if she's ever done any training for the employer before, or whether this was a nurse in charge who showed other people how to do things, or whether this was just a sudden endeavor on her part to be the teacher. So, there are some other facts that might be relevant.

Scenario C

Laura Cooper: The employee is a nursing home residence assistant caring for an elderly patient, who takes some medications that have as a side effect potential mental confusion. The patient has some cash in her drawer, $45, that's been put there by a relative in advance of a resident outing. The money disappears. The residence assistant is accused of stealing the money and has been discharged.

The nursing home resident gets in touch with the fired employee and says, "I'd love to testify on your behalf. I don't believe you ever would have done such a thing. You've been such a good person for me." The union seeks to have that resident testify by issuing a subpoena for her attendance at the hearing. The employer receives a copy of the request for the subpoena and objects to the arbitrator that the subpoena ought not be issued, that it would be unfair to the employer, whose hands would be tied in any effort to impeach the witness because what the nursing home would want to say is that the nursing home resident's ability to perceive and describe is impaired by her medical condition.

So, the argument would be made by the union as to why the subpoena should be enforced. Mr. Cummins?

Brendan Cummins: Unfortunately, I'm not going to be able to make that argument, because this is not a witness I would call. This witness is essentially a character witness whose testimony isn't going to be very probative as to whether the employee stole the money. And the limited probative value of this witness' testimony to me would be outweighed by the risk of putting somebody who's

a vulnerable patient up on the stand to be picked apart by the lawyer of the health care provider that takes care of her. I just wouldn't want to put her in that position. I think it might make us look somewhat desperate to the arbitrator. It wouldn't be necessary, and it would probably backfire. So, I wouldn't call this witness.

If I did really want to call this witness, then I probably would make the argument that the employer's counsel should be put through their paces to do a cross-examination as they would with any other witness whose powers of observation they doubted, which is to just be very rigorous in cross-examining the specificity and clarity of the patient's recollection. I would argue that the patient's medical records really shouldn't be relevant and shouldn't come in.

Laura Cooper: Mr. Kohls?

Timothy Kohls: You start with the fact that this is character evidence only. I think that has to weigh the whole scope of the discussion. But it wouldn't work just to say we could do a rigorous cross-examination. In order to do that cross-examination correctly, you'd have to go into her mental or medical condition, which is really the cause of the mental confusion. And it might not be limited to just a cross-examination of the resident. It might involve testimony from the provider regarding the medication she's taking and the effect of the medication and that she's actually suffering a side effect. So the employer is really left with the choice of doing nothing or being forced into a position where it has to disclose protected health information, which is something it couldn't do. It really puts the employer in an unfair situation. I agree with Brendan that the witness probably wouldn't be called in any case.

One last point is that it does put the employer in a bit of a jam as well. As Brendan mentioned, he wouldn't want to put the patient in a position of having the employer's lawyer sort of pick her apart. We wouldn't want to be in that position either. We wouldn't want to do anything that would put a divide between the patient and the provider. So, it sort of intensifies the dilemma.

Laura Cooper: Would your arguments be different if the particular testimony was more critical? That is, this person was the only witness to some kind of incident, let's say it was treatment of that person, and her ability to testify about that treatment.

Brendan Cummins: I would be much more inclined to call the witness if the witness had direct, first-hand knowledge of the issues at hand. If that were the case and I thought there was no other way to get the testimony, then we might try to call the witness; then

we'd have to deal with the issue of the protected health information. What I would argue is that it shouldn't be disclosed. If the issue is credibility or the powers of observation of the witness, that witness should be treated like any other. Impeachment can be done by rigorous cross-examination.

Timothy Kohls: I think impeachment would be less effective if you can't use the underlying cause of the mental confusion or the clarity of the recall. In order to do that rigorous cross-examination, you'd have to go into things that would be protected health information. If it were critical, we'd be talking about a protective order regarding the testimony.

Laura Cooper: Madam Arbitrator, Ms. Bittel?

Patricia Bittel: You can always have a patient on cross-examination who's confused about whether or not she's confused. So I don't know that her testimony about whether or not she's confused is going to be something on which I can rely. But in any event, if Brendan's not going to present this witness, then I don't have anything to evaluate. I think that's a good decision. It's just a character witness, and there would be other people who would be in a better position to testify to this individual's character than someone that she's responsible for at work.

During our preparation we had an interesting discussion that really relates to what Roberta Golick was talking about yesterday,[56] which spun off of the fact that I've actually done some volunteer work with elderly residents and am sensitive and aware of the dependency relationship between caretakers and the people they're taking care of. I was asked whether or not I would disclose that, and we got into quite a sideline. It really goes to show that, in the health care industry, many of us have personal experiences that we're not going to want to discuss or have had family members who have had health experiences at a facility or otherwise that are very personal, and that may not be revealed.

But in this particular case, if the testimony were critical to proving the case, then we would go back to the first scenario and be dealing with the qualified protective orders. This would be a great case to have that pre-hearing conference call and to talk about some of the issues, because I really don't want some poor, mentally confused witness trying to testify before me.

Laura Cooper: One of the biggest insights that we've gotten from looking at these cases is that parties really need to plan ahead as to

[56]See Chapter 1, "Presidential Address," this volume.

what kind of evidence might be sought. It's very typical for parties, and quite legitimately in most cases, to not focus on preparing a case for hearing until they are quite sure it can't be settled. Sometimes that happens very late in the process. I think that looking at these scenarios has signaled how complicated it can be to sort out an agreement between the parties or to get court orders, and how wise it might be to be thinking way ahead about what protected patient health care information might be needed in a case, and to think about a strategy to make it possible, to get it in where it's critical. Or, perhaps in a case like the character evidence, to make a decision that I better get something else that won't have such a high hurdle in front of it before the information can be obtained.

Scenario D

Laura Cooper: Ellen is working as a registered nurse in the emergency room (ER) and happens to see a co-worker from another part of the hospital, Bill, checking in, apparently as a patient. Nothing looks strange about him. There's no apparent reason why he would seem to be going into the ER. So, Ellen mentions to another nurse, Stacy, that she saw Bill checking in as a patient in the ER.

Later Stacy sees Bill at work and asks him with evident concern, "Are you really okay? How are you feeling today?" Bill realizes that Stacy must have heard from someone in the ER that he had been there as a patient. He complains, saying that that's a disclosure of his personal health care information.

As a result of the investigation that followed, Ellen, the ER nurse, is suspended for five days. The employer has the burden of persuasion on the discipline case.

Mr. Kohls?

Timothy Kohls: This is a clear example of a violation of patient confidentiality. It was disclosure without a legitimate business use. Although we don't have the particular policy, I think that would violate just about every hospital or health care entity's policies regarding protection of patient information. It's true that Bill was visible in the ER and anyone there could have seen him at the admitting station. But at the same time, Ellen learned it because she was working and, therefore, had a duty to make sure that she maintained the information as confidential. Reporting it to Stacy was a violation of that. In this case you have to look at the policy and what the employer has disclosed about levels of discipline

that could be issued, its consistency in applying that policy, and so forth. But you could make an argument that the five-day suspension is warranted. It was an intentional disclosure of protected information without a business reason.

Laura Cooper: Mr. Cummins, what would be your arguments here?

Brendan Cummins: There is a potentially significant notice issue here. Most employees, when they think of HIPAA restrictions, are not going to think of observing a co-worker visiting the hospital. They're going to be thinking about accessing medical records. So in all likelihood, this is a mistake the employee made, not cognizant that it's a HIPAA issue, in expressing concern about a co-worker she cares about, and she is simply unaware that there's a HIPAA issue. For that reason, in all likelihood I would argue that this five-day suspension is excessive, and that it should be reduced to a written or a verbal warning.

Laura Cooper: Madam Arbitrator?

Patricia Bittel: This is one of those instances where lawyers working together are making the world a less friendly and colder place.

There is a notice issue here. This does not strike me as an intentional disclosure. Of course, you'd want to hear the employee testify and get a sense of credibility on that point. But, the scene just strikes me as one employee sees a co-worker and mentions it to another co-worker and forgets that they are in violation of the employer's rules. The employer is right. It does have rules. It does have an interest to protect here. My decision would be that the five-day suspension is way too much. This employee needs to be reminded and at the most something like a warning notice would be adequate for this particular employee.

Laura Cooper: Mr. Kohls, I have a question for you: How clear would the rules be that employees were trained on and how much notice would they actually have in order to know that something like this was prohibited? What do you think?

Timothy Kohls: It depends on the employer. I know at Allina, if you're just reading our policy, and if you use common sense when reading it, then you'd understand that what you learn while you're working is protected information. We saw that Bill was there to seek treatment, not there to visit his co-workers or to do anything else. At that point, his seeking medical care is protected health information. It probably depends, to answer your question, most on the policy that's been crafted. A well-crafted policy would put the employee on notice that this would be a violation of the rules.

Then it goes to the question of how that is communicated. At Allina, there is a lot of effort to make sure that all of our employees go through training at least annually. Those more involved in patient care generally do receive more training on it, but it goes to the notice and the adequacy of the training. In the Twin Cities area, we're probably more likely to be really sensitive to this issue, but I can't speak to other areas of the country.

Laura Cooper: Mr. Cummins, as you've reviewed these sorts of cases, what's been your impression about the kind of notice that the represented employees receive?

Brendan Cummins: I'm not aware of employers having training and dissemination so clear that employees would be aware that this kind of comment would violate the employer's HIPAA policy. Typically, the focus is on medical records, and that's what employees take away from it. Now, there may be other aspects to it. But seeing a co-worker, mentioning out of concern that a co-worker was there, just wouldn't occur to most employees under the information that they're provided. That's just my gut reaction based on what I've seen. I know Tim would very strongly differ based on what Allina does, but that's been my experience of what employees would likely be aware of.

Timothy Kohls: One thing I would agree with you on is that the most common kind of case we see is about the medical record. This kind of thing would be a less common type of violation. It would still be a violation. The most common one is inappropriate access of medical records. And in the days of electronic medical records, this is really easy for a lot of employees.

Laura Cooper: As an arbitrator, I have seen a printout of who was in medical records at precisely what time because the employee's password has to be used and really careful records are kept.

One of the things that we discovered in looking at these questions is that there has been a real enhanced enforcement at the federal level, first with pressure from Congress affecting the Office of Civil Rights, and then that's put pressure on health care providers to be strict in their enforcement. Health care providers have to report to the federal government violations that have occurred, and they have to deal with violations. So, one would anticipate that, as that pressure comes down from above, health care providers are going to be increasingly strict in their enforcement.

There's a question from the audience: Did Bill waive his privacy by going to a hospital where he's also an employee? Mr. Kohls, do you want to respond to that?

Timothy Kohls: As to other employees working at the hospital, no, he hasn't waived it. An employee has the right to seek medical care at the hospital where he works and to expect that his patient information will be kept confidential. I don't think it matters, as a matter of the workplace, whether that changes the analysis. Certainly he would be talking to other people in the ER that night, he'd be disclosing that he was there, but they would have an obligation to keep it confidential.

Laura Cooper: There's a difference between what the law requires and what the employer requires here, as well. HIPAA recognizes something known as incidental violations. I suppose another patient seeing someone in the waiting room is susceptible of disclosure, but it's not, obviously, a violation of HIPAA to allow patients to see other people in the waiting room.

Timothy Kohls: I think that's a fair point.

Scenario E

Item 1

Laura Cooper: Scenario E has six subparts. Our focus here is on just cause and what is appropriate discipline for different kinds of violations of patient privacy. Here we're focusing on looking at patient records, which, as Mr. Kohls has said, is the most common type of violation that's likely to arise. For purposes of discussion, we're going to assume that in each of these scenarios an employee has looked at patient records and that looking at the records is clearly a violation, whether of HIPAA or of employer policy. In each case, the employer has fired every single one of these employees. So the question is: What discipline, if any, is appropriate in each of these cases?

In the first scenario, there's a news story about a local television anchor having been in the hospital ER to be treated for a drug overdose. An employee accesses that record.

The first question is for Mr. Cummins. Do you take this case to arbitration?

Brendan Cummins: No. It's a very easy answer; it's a textbook HIPAA violation. The employee is curious about a celebrity and accesses the medical records out of curiosity. Every HIPAA policy is going to clearly prohibit this. It would be a very difficult case to win, probably impossible, unless the employer was an outlier that

didn't disseminate a HIPAA policy. It's a case that the union would lose.

Laura Cooper: Would it matter what the background of the employee was, say a long-term employee with a clean record?

Brendan Cummins: If the employee was really a long-term employee, say, decades of experience with a perfect record, it's a case we might take just pleading for mercy from the arbitrator. I don't know that we would have any success with that. But the union might take that kind of a case forward.

Laura Cooper: Mr. Kohls, what would be your response?

Timothy Kohls: We would defend this case to the end. If the union decided to bring it forward, this is just the textbook patient confidentiality case. No legitimate business reason. It's just purely out of curiosity to see something that was in the news. This is something for which discharge would be completely appropriate, even for a first offense, regardless of the length of employment.

Laura Cooper: Ms. Bittel, what about the mercy Mr. Cummins is looking for?

Patricia Bittel: In Briar Andresen's paper,[57] she points out some of the enforcement proceedings that have occurred against employers that violated HIPAA, and you're looking at penalties of up to more than $4 million. This is very serious for employers. As a result, we, as arbitrators, need to understand the situation employers are in, and that laxity in enforcing this could really come back to bite them.

In a situation where I have an employer that's jumping up and down about zero tolerance, that is a situation where I would nod and say, "Yes, I understand zero tolerance," and would uphold the discharge even on a first offense. If you're dealing with a 25-year employee, we can take a look at that. But, I understand that this is a very serious matter for employers and it's only getting to be more so.

Certainly, you want to look at the environment and the kind of penalties that have been given in the past, but one employer's world is not the same as another's, and not every employer is necessarily zero-tolerant. If it's not, then I'm not either. But, that's how I would go at it. It's to see if this employer is particularly concerned, afraid, and protective.

Laura Cooper: Ms. Bittel mentioned the dollar amount of fines. It just seems to me to be an opportunity to once again caution

[57]See Part I of this chapter, "HIPAA Basics for Arbitrators."

arbitrators that if you do have possession of health care information that is protected by HIPAA, covered by a protective order, that it's really incumbent on you to take extraordinary precautions to secure that as best you can.

One of the million-dollar fines involved an employee who took records home and left them in a subway car, and they were never found again. An arbitrator rushing in a taxi to the airport creates a bit of a horror story in that regard. But these files are different files. We do have a special obligation to keep them secure. As much as we typically have a practice of destroying records after arbitration cases, one would want to, again, take particular care to follow the terms of a protective order and destroy any record.

Patricia Bittel: I would go so far as to say that if you do have patient personal health care records from a file, where the parties have been sensitive to this issue, it really behooves you to either send those back or confirm in writing that they've been shredded.

Laura Cooper: That sounds like a good practice.

Item 2

In item 2, the employee accessed her mother's records but didn't have a signed release. But, she nevertheless did so at the request of her mother, who said she wanted the daughter to check on her blood test.

Mr. Kohls, what about here?

Timothy Kohls: In all of these cases an important thing to consider is this: What exactly does the policy say? How effectively has it been communicated, and how consistently has it been enforced? In this one, depending on the policy and the communication, you can make a good argument that the employee accessed confidential patient information without authorization. That violates the rule. In which case, discipline would be warranted. There are mitigating circumstances in this case. For one, it appears that if she had just followed the rules, she eventually would have gotten the proper authorization. Perhaps you could make an argument that a lesser form of discipline would be warranted. But it then goes back to what does the rule say, how has it been communicated, and how has it been enforced?

Brendan Cummins: A discharge is very excessive here. We have an employee disclosing to a patient at the patient's request. That certainly doesn't warrant a termination. There may be a technical violation here because of the absence of written authorization,

but I would say a discharge certainly doesn't fit the crime here. The discipline should be reduced maybe to a written warning.

Laura Cooper: Ms. Bittel?

Patricia Bittel: She did what her mother told her to do.

Brendan Cummins: She deserves a medal!

Patricia Bittel: There are those of us who are parents who want to adopt this woman!

There are mitigating circumstances in this case. She had a legal right to request and receive the information to which she gained access. The patient had notice and gave express authorization, even though it wasn't in writing and wasn't in accordance with the employer's particular procedures. So, I would be influenced by the fact that there really was no violation here of the statutory intent, or even of the employer's intended protection. Were the violations only technicalities? There's no way that I would sustain the discharge.

Laura Cooper: Mr. Kohls, in a case like this, there's a challenge to the employer's advocate to overcome the common sense of the arbitrator by suggesting that in this case a technical violation should be grounds for discharge. How do you make that argument?

Timothy Kohls: There are a couple of things to think about in that regard. One is what you talked about earlier, about the million-dollar fines that are going out and the incredible amount of risk that covered entities have when dealing with protected health information, and that even a technical violation could result in a severe penalty to the employer.

Another is that we put these systems in place to protect the integrity of the whole system, so it's not for an individual employee to say, "Well, I would have gotten the authorization if I had just gone through the works. So I'm just going to do it." There's an element that the system only works if we maintain the integrity of the whole system. Even though in this instance you could say it's just a minor issue, it could have broader ramifications.

Laura Cooper: Did you want to defend common sense, Mr. Cummins?

Brendan Cummins: Well, a foolish consistency is the hobgoblin of small minds. I think consistency is important, especially with HIPAA. But we shouldn't apply the protections and regulations without an eye toward the specific facts of the case. That's what just cause is all about—looking at the specific facts, the totality of the circumstances, and how much at fault the employee is. So, I

don't think it's justifiable to discharge someone because there's a technical violation of HIPAA. Under the just cause standard, you really have to look at the degree of fault of the employee.

Laura Cooper: Mr. Kohls, I'm aware that Allina has a policy that provides gradations of discipline for different kinds of violations and specifically deals with a sort of benevolent breach to put the employee on notice that even well-intentioned inappropriate access can be subject to discipline. Do you think that helps to make the case that a technical violation matters and communicates to employees that benevolent access is still unlawful? Can you say something about that policy?

Timothy Kohls: At Allina we have a couple of different policies. One is our general employee policy regarding confidentiality of patient information, and it would say that this disclosure violates the policy. We would then break down the severity; I think the term we use is a "manager guideline" for when violations happen. So in this instance we would say there was a violation. She obtained or accessed the information without getting the appropriate authorization. During the investigation, we would look at how severe a penalty is appropriate under the circumstances.

We look not only at the intentionality or the severity of the breach but also at the employee's work history and the other factors that you would consider in a just cause analysis. But we do break out a little bit. In this one, I think it would be an intentional access, but it was not following procedures versus curiosity or some other sort of bad intent. It would be mitigating circumstances in this instance where the employee could have obtained the appropriate authorization and didn't. I can't say for other employers, but that's the policy that we have.

Laura Cooper: You mentioned these managerial guidelines to tell supervisors when to issue discipline and what kind of discipline. To what extent are those levels of violations communicated to employees?

Timothy Kohls: The level itself, which contains examples but nothing ironclad. The managerial policy is not for general dissemination to all our employees. Our policy itself has a very long, although explicitly nonexhaustive, list of activities that would violate the policy.

Laura Cooper: It seems one of the challenges with these disparate kinds of violations, especially in a large institution such as the ones you're responsible for, is the matter of consistency. It's certainly persuasive if a union can say that other people were given

different sorts of discipline. To what extent are you able to obtain records to keep track of different types of violations and consistency of discipline across those violations?

Timothy Kohls: I can't say how far back it goes, because I haven't been at Allina for that long, but we keep records of everything. All of our patient confidentiality investigations are handled and recorded centrally. So it's not just an individual hospital or entity doing anything, it is our central office tracking everything that happens. We have developed levels, with the people who are responsible for investigating and making decisions, to make sure that the levels we've assigned are part of the whole, so we do make sure that decisions are made consistently. It's actually a fairly important thing that we've worked on over the past few years.

Item 3

Laura Cooper: In item 3, four years ago the employee's mother was hospitalized. At that time the mother signed a release allowing the employee to access her medical records. But now that signed release has expired. Such releases typically have an expiration date. The mother now comes back to the hospital and the employee now accesses her records, but there is no new release.

Mr. Kohls, what's the discipline here? Was the discharge appropriate? Are you going to defend it?

Timothy Kohls: You can take this a couple of ways. But I'll say the discharge was appropriate. The employee obviously knew the rules. She obtained authorization a couple of years ago when her mother had been admitted previously. So it's quite clear that she understood that she needed to have authorization to access the information. In this case, it was a breach of patient confidentiality for her to access her mother's medical records without the appropriate authorization. Then it goes back to the other factors as to how well that rule was communicated and how consistently it was enforced. But I think you could make an easy argument that the discipline is appropriate.

Laura Cooper: Mr. Cummins?

Brendan Cummins: This looks to me like another technical violation. There was a release. It's expired. It's not clear that the employee was aware that the release expired. It may just be a mistake. If that's the case, then the discharge certainly is inappropriate. Perhaps the employee should have done a better job of

making sure that the release was still effective. Some level of discipline is appropriate, but certainly not discharge.

Laura Cooper: In the previous item, the mother asked the daughter to access the records, and here there isn't any similar request. Does that make a difference to you?

Brendan Cummins: It makes the case a bit less compelling, but there was a release. Under the facts stated here, there was a release in place. It simply expired. So, my view of this is, if the employee was unaware of the expiration and simply made a mistake, then the level of discipline should be reduced.

Laura Cooper: Ms. Bittel?

Patricia Bittel: Like any arbitrator sitting out here, you're wondering: What did the employee know about the expiration? Did she think it was still valid? Had she just forgotten? Or did her testimony look a little guilty? Did she actually seem to know? Had she been reminded recently in training that all releases have to be recent, and how recent? What does the policy say? What did the training materials say? There are a lot of things that could influence the outcome in the case.

If I were persuaded that the employee genuinely forgot that the release had expired, that would be a mitigating circumstance. I'm looking at whether or not this employee is employable. If, on the other hand, she was flaunting the regulations that apply here, I'd be deeply troubled by that and much less generous in how I would view her situation. So it's a little hard for me to answer this because in a real hearing there would be a lot more to go on. But, generally speaking, this situation is more egregious than the one where the mother asked the daughter to take a look at the records. So, I am looking at either sustaining the discharge or changing it to a suspension, but it wouldn't be just a letter of reprimand.

Item 4

Laura Cooper: This fourth item got added to our list by Mr. Cummins, who has encountered rules that prohibit employees from accessing their own electronic medical records. Do you want to say something about such a practice?

Brendan Cummins: Believe it or not, I've actually seen this type of policy. The employer's rationale is: If you don't have a legitimate business reason, then you can't access a medical record, even your own. I would argue that this is not a reasonable work rule.

An employer doesn't have a legitimate business reason to prevent an employee from accessing his or her own medical records. It's simply the desire for consistency of protocol. You've got to have a legitimate business reason; if you don't, too bad, even if you're the patient.

I think this points out the importance of adherence to just cause and reasonableness, even in the important area of HIPAA. A policy against access without a legitimate business reason shouldn't be applied overzealously in an instance where an employee accesses his or her own record.

Laura Cooper: Mr. Kohls?

Timothy Kohls: First, maybe we should point out I don't think this is a HIPAA violation. This is a policy violation by itself. I would tend to lean toward saying that discharge would be too severe in this situation, although I do go back to the point that it's not for the employee to decide to access information without following the rules. The rules are in place to protect the information of all our patients. We have a legitimate expectation and the right to think that our employees will follow those rules. In this situation, if we have a policy that's clear enough and it's been effectively communicated, you can make the argument that the employee should be disciplined. The employee doesn't get to choose to not follow the rules.

Laura Cooper: Ms. Bittel?

Patricia Bittel: During our discussions preparing for this session, I asked Tim, "What is the business interest that's being protected by this rule?" We had a bit of a discussion about that. He can address it better than I can. But as I recall his viewpoint was that we have to have procedures in place, otherwise we don't have enough control over the dissemination of information or access to the system. So, that's fair enough. That's an answer. They do have to regulate access into their system and who has access to medical records.

But their regulations are designed to effect HIPAA protection. HIPAA protections have two goals. One is to protect, first of all, health information from getting into hands that the patient has not authorized. The other is to guarantee the patient's access to his own health information. I'm sensitive to that. I understand that these rules are guarding the access point, and that's valid. I certainly wouldn't uphold this discharge, however, because the rules, if they track HIPAA, should have a provision for employees to access their own information. I'd want to look at that and see

how far afield of that procedure the employee actually went. Even if he was far afield, he did have a legal right to this information. It's very protective for the employees, and I don't see discharge as an appropriate approach to this situation.

Laura Cooper: There are really two parts to HIPAA. HIPAA is trying to protect the privacy of patient information, but the other half is to ensure patients access to their own information. So it's a really good argument here, I suppose, about reasonableness based on that other prong of HIPAA.

Timothy Kohls: We ended up talking about the privacy way more than access. From our line of work, I think we would say that this employee would have access to his medical records by just following the appropriate procedures.

Laura Cooper: As a patient.

Timothy Kohls: As a patient. And we have separate policies and procedures for our patients to access their information. That would have been the appropriate way for the employee to go in this instance.

Item 5

Laura Cooper: In this fifth item, the employee and her father are estranged, but she's nevertheless sincerely concerned about his welfare when she learns that he's been hospitalized in the very place where she works. So, she looks at his medical records four separate times to see how he is doing. Mr. Kohls?

Timothy Kohls: This is another one where it's intentional access without a legitimate business reason. The fact that she's looking at her father's record is not a mitigating factor, and the fact that she did it four times compounds the case.

Laura Cooper: Mr. Cummins, how do you want to defend that case?

Brendan Cummins: It's a difficult case to defend, because it is intentional access. It's an intentional violation. I would argue that there's a mitigating factor here because the employee's motives are sincere rather than malicious and would plead for mercy on that basis, and look for other mitigating factors.

Patricia Bittel: You probably would need to find some more mitigating factors. To do it four times is an aggravating circumstance in my view, and it's really not compensated for by the mitigating circumstances in this case. But if you found some more mitigating circumstances, we could take a look at it.

Laura Cooper: I would just say that there might be aggravating circumstances, too. I had one case in which, after discharge, an employee discovered that her password still worked and accessed records thereafter. That did not help her case.

Item 6

Laura Cooper: In this sixth, and last, item, it's the employee's ex-husband who's admitted to the hospital. It's been a contentious divorce. She's hopeful that there might be something in his medical record that she could use to try to deny him visitation with their children, so she accesses his medical records without permission. Mr. Cummins, do you want to take that case?

Brendan Cummins: No, no. I would refuse to take it, even if they paid me to take it. I can't defend it.

Laura Cooper: People argue that every discharge case is taken to arbitration for reasons of the duty of fair representation. Do you want to disabuse us of that belief?

Brendan Cummins: There would be no duty of fair representation risk here. You'd be well justified in not taking this one forward.

Laura Cooper: Have you had to arbitrate such a case, Mr. Kohls?

Timothy Kohls: Not in my tenure at Allina have we had to arbitrate this case. We have had others that have been high-profile media cases, but nothing that I've seen along these lines. It looks like this item has the same pattern as the last one, but without the benign motive of the daughter. If this is the case, then I think it's a pretty clear-cut discharge.

Laura Cooper: Ms. Bittel?

Patricia Bittel: I have friends who strongly advise me that in the world of mitigating circumstances, revenge against any ex-husband should be seriously considered. Notwithstanding that, I don't think it would be enough to avoid discharge in this case.

Laura Cooper: [Responding to a question from a state government labor relations attorney.] There's an article in the *Star Tribune* from last month involving a Mayo Clinic employee who accessed the medical records of her boyfriend's suspected girlfriend to find out if the suspected girlfriend's pregnancy might be attributable to her boyfriend.[58] The employee was prosecuted

---

[58]Paul Walsh, *Medical Data Snooping Admitted—Ex-Mayo Worker Is Sentenced for Spying on Her Romantic Rival,* STAR TRIBUNE, May 16, 2012, *available at* http://twittweb.com/suspicious+boyfriend+a+-20544429 (last visited February 16, 2013).

in federal court, pled guilty, and was sentenced. I don't think you would be comforted by the last line in the article. It says, "The mother of two lost her job at Mayo over the invasion of privacy. She now works in state government."[59]

I'm restating a question from Catherine Harris: Arbitrator Harris' question is whether an arbitration award that discusses a grievance involving patient care could be a HIPAA violation. The first question is whether you are a health care provider or a business associate. If you're not either one, then you're not subject to the law. The other thing would be whether you have de-identified the information such that it wouldn't be private health care information. Mr. Kohls?

Timothy Kohls: I think that you covered it. First of all, the requirement applies to covered entities under the statute and the regulations. Clearly, health care organizations would fall under that category. The business associate we talked about before would also be covered under it. I don't think that an arbitrator who hasn't signed a business associate agreement would be covered. As we talked about for the last hour or so, in the presentation of the evidence and the use of the evidence, we would be using protected health information. One thing to consider is this: Would the ultimate award be covered under a protective order to some degree if it has to get into the details of the provision of care?

Laura Cooper: So, it might well be covered in the protective order itself.

Patricia Bittel: This is a great subject of conversation with the parties. If in the course of writing the decision I found that I could not render this decision with de-identified information, then I would get on the phone to both parties in a conference call and say, "Look, I can either have a very cursory decision, or we can deal with the fact that my decision may have information in it. How do we want to deal with that?" We may have already dealt with it because I have sensitive information.

Laura Cooper: I have a number of take-aways from this inquiry that we've just been engaged in. One is make sure to look at specific state laws as well as federal laws. Start early if there's any chance that patient record issues may be raised. Be aware that in some cases an arbitrator's subpoena is not enough or may not be enough and that court orders may be necessary. To try to de-identify records—not the kind of redaction that we've been used

[59] *Id.*

to—pay attention to the list of what needs to be taken out for de-identification.[60] And very carefully secure any patient records that you may have. Are there other take-aways?

I'm restating a question from Lisa Kohn: Arbitrator's Kohn's question is whether you can create a document that's not a patient care document but that stipulates critical facts. And I think you are right that it is very important to suggest that the dates have to come out. Because even putting a year in a document, not even a more specific date, is problematic under the statute. Do you think that would work, Mr. Kohls?

Timothy Kohls: I think, potentially, it could work. I think you'd have to look more beyond dates and other things. There's a whole list of 20 or so items that would have to be excluded,[61] and then you have to look at whether you have anything useful after that.

Laura Cooper: Thank you very much for your attention. We appreciate it. Thank you. Good afternoon. And thanks to our panel.

[60] See Part I of this chapter, "HIPAA Basics for Arbitrators."
[61] *Id.*