Implications of Internal Data Theft at Hospitals: Tips for Preventing and Handling Data Breaches by

Internal data theft by employees at hospitals and health systems is becoming an increasing concern. Criminals are targeting low-level employees who have access to patient information at the hospital for the purpose of stealing the data for profit. What should you look for if you are trying to root out a potential data breach or prevent these kinds of breaches? What steps should you take if a breach occurs?

Data security and privacy attorneys Gavrila Brotz and Marissel Descalzo provide tips for uncovering data breach threats, best practices for conducting an internal investigation, what to do when a breach occurs, preventive measures, and cyber litigation trends in this 20-minute *Carlton Fields on Cyber* podcast.

TRANSCRIPT

Marissel Descalzo: Thank you. Recently there's been an increase in internal data theft. Data breaches are not just the result of external threats. We are seeing an increased trend in hospital and health system employees who are now fully accessing and stealing patient information. The purpose of this is to sell the information and the reason is, it's very profitable. Criminals are targeting low-level employees who have access to patient information such as people in the medical records department; transporters; people in admissions. Most of time these individuals are either already employed by the hospital or some may be seeking employment for the specific purpose to assist these data breach thieves.

We've seen positions that have been targeted either hospital-based or even people seeking positions with third-party vendors in order to get access to this information.

Gavrila Brotz: So what do you look for if you are trying to root out a potential data breach or prevent these kinds of breaches? Look for numerous general searches that are being performed by hospital employees or employees of vendors, searching for patients' names or their dates of birth. Numerous successive searches in modules that provide you with demographic information without entering into a patient's record or high volume of printing of demographic information or financial information of patients. For example, their face sheets or other screenshots with patients names, addresses, dates of birth and/or their Social Security numbers. It's very common that these data breaches are ultimately found when an individual is pulled over by the police for a traffic stop and the policeman notices a large stack of face sheets from a hospital and it turns out that that's what's been going on. So the key is to find this *before* the traffic stop, to find this internally by seeking out and finding these kinds of searches or printing that's going on by employees. So you want to identify them and investigate.

Some additional preventative measures that you can take are to prohibit employees' access to patients' full Social Security numbers, as much as possible. And you can also restrict employees by requiring all of their personal belongings, including their own phones or devices, to remain in a secured area to be retrieved only before they leave and to have them sign and execute acknowledgments verifying their attendance at routine HIPAA training and that also acknowledge their understanding to abide by regulatory requirements. As far as vendors are concerned, it's important to limit their employees' access to information or entire modules that are essential for the performance of the vendor's job duties. And they should also be required to execute agreements, which indicate their acknowledgement and compliance with HIPAA requirements and require them to be responsible for safeguarding any information that can be extracted from the computer system.

Marissel Descalzo: Once you recognize you have a problem, the next step is probably conducting an internal investigation. There's top rules that every institution should follow when they're conducting an internal investigation. The first thing is decide whether the internal investigation will be conducted by in-house counsel or by outside counsel. The next step is whether you have to issue a document

hold, or a litigation hold sometimes it's referred to, and whether you need to stop the destruction of certain documents. You need to get with your IT department to discuss this. You need to narrow the scope or identify the scope of the investigation and then narrow the scope of the investigation. You don't want to do a broad sweeping investigation in the event there is a later criminal case or class action that would require disclosure of all this information and maybe it's things that your institution does not want to disclose.

Be very mindful of the attorney-client privilege. Lines are often blurred when you have an internal investigation. You also have to be mindful of conflicts that arise when you are conducting an investigation. And finally, you have to decide whether you are going to disclose the results of the investigation.

When you are investigating, you need to determine whether you are going to actually interview that employee or that vendor's employee whose been identified by an audit as an outlier, as a person that may have conducted or performed illegal or improper searches. If you do decide to interview this person, you have to be mindful that during that interview, a conflict may arise and that person may have a right to their own representation. That is why it is often important to consult with outside counsel when you are making these determinations and you are conducting your investigation.

Now once your investigation is complete, you have to decide whether you are going to make a referral to the authorities or not. There are some advantages and disadvantages of doing that. The advantage of course, is it sends a message to your institution that this type of behavior will not be tolerated. Getting law enforcement involved also helps bring the wrongdoer to justice and maybe the institution will feel vindicated by that. The cons are that you have all of the sudden created a record for some litigation in the future and you have probably admitted that the institution has some culpability in the breach because maybe their controls were not in place properly or whatever it may be. So these are all things that have to be considered when you are deciding whether to disclose or not.

By way of example, here is a hypothetical of how these data breaches often come to light to institutions. A risk manager receives a call from local law enforcement advising that 20 face sheets from your hospital have been recovered from a vehicle during a search incident to the arrest of an individual. What does the risk manager do next? Probably the first thing they should do is call in-house counsel and decide how they are going to handle this. In-house counsel should decide whether they are going to hire outside counsel or not. You should probably get on the phone with the IT department and have them start running audits and then you have to decide whether you are going to conduct an internal investigation. At this point, disclosure is probably been decided for you because law enforcement is involved, but you still need to go through the steps of the internal investigation to assist law enforcement in deciphering who could have done this from within the hospital to prevent future breaches, and you also want to assist law enforcement in doing this

because you do not want to seem combative with them and you do not want the institution to appear to be part of the problem.

Now if there is a pending law enforcement investigation, you have the ability to delay notice to victims of a breach. This is a good tool for institutions to use when there has been a data breach at your institution. If there is a law enforcement investigation that would be impeded by notice to victims, law enforcement can give you a 30-day delay. The initial request for 30 days can be made orally. The entity should document it in writing regardless. If you want a second delay or if law enforcement needs you to delay an extra 30 days, that request must be in writing from law enforcement.

Another hypothetical for you to consider is what if law enforcement contacts Risk Management advising them they would like to set up surveillance at the hospital to catch the thief in action. What do you do? That is something you need to seriously consider. Having law enforcement conducting surveillance in your hospital, probably not the best idea. Something you could do is say "We'll conduct a surveillance for you. We'll review the videos for you. We'll focus the cameras on the area that you want to look at and then we will provide you the relevant video clips." You might question whether it is a HIPAA violation to have the police in there doing surveillance. It could be even though they have a law enforcement purpose for doing it, when they give you a subpoena or even a search warrant, they can get around the HIPAA rules. But it is still something to consider because other patients' information is going to be probably compromised and maybe that is something you can bring up to law enforcement.

Gavrila Brotz: Okay. So a breach has occurred. Law enforcement is potentially investigating and now you are required to notify the government and individuals depending on the scope of the breach and whose data was exposed and where they are from. One thing that we see, especially with hospitals, is that the patients can be from all kinds of places. For example, we are located here in Florida and patients can be visiting here from all over the country and if their data was exposed, the hospital now has to comply not only with federal law and Florida state law, but the state laws of every patient based on where they reside. So you could wind up having to do notifications in something like 40 different states. And unfortunately, there is not yet any real uniformity between the states rules on notifications. Fortunately, we have a nice survey available online which shows the general differences between the requirements. That can be a useful guide to find out what your exposure is and whether you are required to provide any notice, for example, to various states' attorneys general as well as notices to the individuals themselves. Keep in mind also that the definition of the breach itself can vary state to state. So first you will have to determine if what happened in your facility is even a breach as defined under certain state's laws and then if you would be required to provide any notice to the state's government itself. And also bear in mind that if an individual is now deceased but that individual's data was exposed, you will still be required to provide notice to that individual's next of

kin or personal representative of the decedent's estate if you have their contact information. So you also must bear that in mind.

The next step to consider is how to word the notice that you are sending out to the individuals. It should be consistent with the OCR (The Office of Civil Rights Report) and any state agency notice, so whatever is required to be in there of course must be. But the words should also be chosen carefully. We see that in ultimate litigation, when there is a class action based on a data breach, Exhibit number 1 to the Complaint is a copy of the notification letter that went out. So it is important to craft it carefully bearing in mind that it could be Exhibit 1 in future litigation.

We have also seen that when offers are included in these notices to, for example, provide free credit monitoring services for a year, that that can ultimately be good or bad. It can provide a lot of good press and goodwill for the individuals who receive the notice. When there have been massive data breaches and that offer is not provided, it can become a critical relations issue for the company for not doing it. However, we have seen that at least one court has found that that offer constitutes an admission that a harm occurred so it is something to consider carefully. In addition, in the notice, if there was any delay pursuant to a law enforcement investigation, you might need to specify that in the notice to explain why the notice is going out on whatever date if a data breach occurred and was discovered quite a while before.

Now the Office of Civil Rights automatically investigates every breach that affects more than 500 individuals in a particular state or jurisdiction. OCR also has the discretion to open investigations for breaches affecting less than 500 individuals. So you will need to prepare for a potential OCR investigation if a data breach occurs. We recommend convening an internal task force of individuals and determine who will gather and maintain documents, who will ensure compliance with regulations and who will assess and perform internal risk analysis. This can help mitigate the risk of a future data breach and it will help you adopt a corrective action plan. That plan should assess how the breach occurred and how to prevent such a breach from occurring in the future. It should plan to implement those changes to remedy the problem that created the breach and it should document all of the corrective actions that you are taking.

You should ensure that your risk analysis required under the security rule is up-to-date. That is an assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of that electronic protected health information that is held by the hospital. As much as you can, maintain the attorney-client privilege over the investigation of the breach. And that means that the more you can work with outside counsel, the better. We are seeing plaintiffs argue that these investigations should be subject to discovery in litigation, meaning that all the records of these investigations should be turned over to the plaintiffs because this is part of a routine reporting requirement and not something that an attorney is really weighing in on. So the more you can

insulate these investigations and protect them and keep them privileged, the better. And you do that by not only working with internal counsel, but then outside counsel adding extra layers of protection.

You should also perform audits to ensure that potentially infected individuals have all been captured. Sometimes when a data breach is first discovered, you think that, for example, 500 people had their data exposed and we recommend continuing to audit to make sure that you really did capture the full scope of the breach. And it's okay if you didn't because you can update OCR and you should not delay reporting to OCR to make sure that you have captured the whole field. Report to OCR with what you have and then continue to audit and you can update them if the scope of the breach was larger than originally anticipated.

So, now, OCR has investigated. You have had your data breach. You have worked with law enforcement. You have notified individuals. What comes next? Often, unfortunately, is litigation. There is a new trend to get a class of plaintiffs together and file the claim against not just hospitals, but various entities that have had a data breach. Why not go for some money. And so as I described before, we see Exhibit 1 to a Complaint is the notification letter and the allegations are generally, "I was harmed because my data was exposed." Some complaints really just only state that – that there is an inherent value in personal data and if it is exposed, the person whose data was exposed, was harmed. That is generally unsuccessful in court. To bring a claim, you first must have standing, which means that you have had some kind of harm that can be redressed by the litigation. And courts rather consistently find that just having your data exposed is not enough of a harm to bring a case against an entity where there was a data breach.

Also, we see cases where plaintiffs allege that not only were they harmed by having their data exposed, but they are now afraid of future identity theft or false charges on their credit cards based on whatever data was exposed in a breach. And those cases are also generally unsuccessful, though it depends on the circumstances. The Supreme Court of the United States weighed in on this but not really in a data breach context. It gave some general guidelines on standing. And it's been interpreted differently in the courts, but the general rule is that a mere fear of a future identity theft is still not enough of a harm to give you standing to bring your claim.

There was recently a decision from the Seventh Circuit Court of Appeals in a case against Neiman Marcus, the luxury retailer which had a large data breach, where there is a class of 350,000 plaintiffs, 9,200 of those plaintiffs actually had false charges to their credit cards. And so the court found that actually the entire class of 350,000 people really had a future fear that was credible of false charges to their credit cards or identity theft because it had already happened to 9,200 of them. And so that court found that those plaintiffs had standing to bring a claim. The court did not address whether the case could also be dismissed for other reasons. And the court also specifically found that there was no just pure inherent value in data, the exposure of which provides enough harm to bring the claim. But still, it shows that this area of law is developing and as more and more

courts weigh in and create more and more decisions, it is a more complex field to navigate and until the U.S. Supreme Court weighs in, if they do, in the future there are a multitude of decisions out there to consider.

Another new trend that we are seeing in claims against hospitals, and not just hospitals, is that plaintiffs are not alleging that they are afraid of future identity theft, but rather that they had a contract with the hospital that was breached when the data theft occurred. So their argument is that when they showed up at the hospital and paid for their medical services and they signed their conditions of admissions form, that was not just a contract of payment for medical services, but rather a contract of payment for medical services plus data protection. So when the data theft occurred, or the data breach occurred, therefore, there was a breach of the contract. These cases generally are very unsuccessful. They have also been tried in the non-health care context. For example, the Chinese food chain, PF Changs, was sued when they had a data breach. The argument was very similar. The plaintiff said, "I didn't just pay for Chinese food, I paid for Chinese food and data protection." And the court really did not find that to be credible. You are really just paying for Chinese food. And the argument in these cases, on behalf of the hospitals, is no, you paid for medical services, that is what hospitals provide. You are not contracting for an additional layer of data protection. But it is a new trend that we are seeing in claims against hospitals.

Now claims that tend to be successful are when there are proven losses. For example, in claims against retailers where customers' credit card numbers have been exposed, banks that have had to ultimately pay out and cover false charges can absolutely bring claims against the retailers because they really have had a harm, they have paid out money. And so those claims are at least successful enough to survive the standing test.

So those are the trends that we are seeing in litigation. And I think that the ultimate takeaway from this is to involve internal and outside counsel as early as possible when you have a data breach so that you can mitigate the harm and hopefully stave off future litigation or handle it and nip it in the bud.

So with that, thank you for joining us today. Marissel -

Marissel Descalzo: Thank you.

Gavrila Brotz: Thank you.

specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.

Related Practices

Health Care
Cybersecurity and Privacy

Related Industries

Health Care