A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

MAGAZINE

JANUARY 2019

Workplace violence: What compliance professionals should know about the unthinkable (P18)

Controlling mobile devices in an academic medical center: Unique challenges (P22)

Compliance tips for implementing an electronic medical record system (P28)

Tried and true survey readiness (P34)

GREG RADINSKY
SENIOR VICE PRESIDENT &
CHIEF CORPORATE COMPLIANCE OFFICER
NORTHWELL HEALTH

SEEING ENFORCEMENT ISSUES FROM ALL SIDES

(P12)

HCCA™

CONTROLLING MOBILE DEVICES IN AN ACADEMIC MEDICAL CENTER: UNIQUE CHALLENGES

by Marti Arvin

Marti Arvin

(marti.arvin@cynergistek.com) is Vice President of Audit Strategy at CynergisTek in Austin, TX.

bit.ly/in-MartiArvin

In today's healthcare environment, mobile devices are rampant. Controlling the nature and method of data stored on these devices is not easy in most industries—and mobile devices in the healthcare environment present a unique challenge. What makes securing mobile devices particularly difficult in healthcare and even more difficult in the academic medical center (AMC)? It helps first to understand the environment.

The academic medical center

The old saying is that, "If you have seen one AMC, you have seen one AMC." The organizational structures, politics, and cultures vary among AMCs. The nature and structure of the legal entities involved can also vary, but there are consistent factors. Usually, there is a healthcare facility, such as a hospital, and an AMC will have faculty members and trainees (i.e., residents and students). The clinical activity of the faculty members will often be performed through one or more faculty practice groups. Clinical research is often also being conducted simultaneously on the university side. Regardless of the structure, controlling the data on mobile devices is difficult, but sometimes the AMC structure can make an already complex proposition even worse.

So, what are some of the variations of the structures? There can be a single legal entity in which the university owns the hospital and faculty members are employed by the university, both as educators and clinicians. All research activity is performed by that legal entity, and most of the training programs are all conducted by the entity.

Another variation is that the university is one legal entity responsible for most of the training programs and research activity, and the health system is another legal entity or a combination of related legal entities. Yet another variation is a combination of the first two (i.e., one or more of the hospitals are a component of the university and the health system owns others) where all entities share common governance and oversight.

There may also be one or multiple affiliated hospitals that are each an independent legal entity with a separate governance structure. One or more faculty practice groups generally employ the physicians. The faculty practice groups may be affiliated but separate from the university. A practice group may be a component of a large health system or completely independent from it. When the practice group is a separate legal entity from the university, the faculty members are generally dual-employed. They are university faculty performing educational and research activities for the university while, as clinicians, they are performing patient care services through the faculty practice group.

Mobile devices in these environments

What are the implications for mobile devices? Most physicians do not want to have two of everything (e.g., phones, computers) for their clinical work and faculty/research work. Many universities and some health systems don't want to buy computers for everyone. If the university or the health system supplies the devices, the brand of the device and the features on it are often not the most high-end. If the organization supports Apple devices but the end user prefers Android, it usually results in a bring-your-own-device (BYOD) structure. And if the university or health system does not provide the device at all, it leaves only a BYOD structure.

Securing devices the AMC doesn't own

The perfect solution doesn't exist, but there are ways to control what data can be stored on certain devices. The first step is to start with a policy. This simple solution is likely the least effective, but it will establish the foundation for all other controls. An organization can have a policy stating that no sensitive data, such as protected health information (PHI), personally identifiable information (PII), or proprietary information, can be stored on a mobile device unless it is encrypted. Enforcement of such a policy would be next to impossible without other controls.

The organization can use a technology solution to help ensure data is protected. The solutions will vary depending on the device and method of protection. Many technology solutions will support different types of devices. For example, the organization may set up the network and servers so that only registered laptops can be connected. These controls, typically certificate-based, will allow the device to be remotely managed and can ensure a password standard, patch level, and encryption are enabled. It is also important to have a remote-wipe capability if the device is lost or stolen. These controls should be defined by the organization and be leveraged as the minimum threshold to permit connections.

Portable external drives present a significant risk because of the high probability and impact of loss. Again, technical solutions can encrypt all data saved to such a removable drive. This effectively mandates the encryption "safe harbor" solution to prevent a data breach; however, it may not be a solution in every instance. If a mobile phone is connected as an external storage device, the technology solutions may not encrypt the data going to the phone. Additionally, these solutions may not secure files created on the external drive. Other technology solutions can evaluate the external drive when it is plugged in to the computer to ensure the device is encrypted. Some organizations have taken the step of disabling the USB drives on computers before they are deployed to the workforce and only allow the drives to be enabled on an exception basis. This would only work if the organization supplied the computers to its workforce but, in a BYOD world, that solution would not work.

> **The perfect solution doesn't exist, but there are ways to control what data can be stored on certain devices.**

In a BYOD environment, these solutions come with more baggage. These same issues occur if the organization considers providing encryption software to end users for their personally owned devices. For example, does the organization's license for the software permit it to be loaded on a device not owned by the organization? What happens if the individual's computer is somehow damaged or corrupted by the process of installing the software? What if the user has not kept up to date on system patches? What if the individual's computer is incompatible with the version of the encryption software the organization is using? What if the health system wants to provide encryption software, but the device is owned by the university? What if the end user objects to the technology solution for privacy reasons?

The organization may also choose to provide encrypted external drives for users. But what happens to those drives once the user, such a resident or student, is no longer with the organization? What happens to the organization's data that is on any of the devices discussed thus far? Organizations need a process for getting their own devices back and ensuring only data that is approved can go with the user when the user leaves the organization.

Organizations may consider requiring an attestation from any user who had access to sensitive information when that user leaves the organization. In that attestation, it can state that either the user has no sensitive information or that any sensitive information they are taking has been approved by the appropriate authority and is now their personal responsibility. If the user refuses to sign the attestation, the organization can document this and inform the user that any sensitive data that is removed from the organization will be considered a theft.

Most of these are issues that any hospital, physician group, or other provider may need to deal with regarding the security of mobile devices, but what makes it more difficult in an AMC? First, as previously discussed, there can be multiple legal entities that have various concerns. Each entity may have different risk tolerances, different budgets to support the end user, and various controls to help protect data. When there are multiple organizations, the effort to secure mobile devices needs to be coordinated and easy to follow by the end user. If the hospital has one policy, the university might have a slightly different policy, and the physician practice group could have yet another policy. With multiple policies to follow, the user who works in all three entities will find it difficult to be compliant with all of them. As a result, the risk increases that the user will follow whatever policy they find easiest, which is typically the least restrictive policy or something they make up.

Academic freedom

Another unique challenge in an AMC is the concept of academic freedom, which is the premise that says faculty and students should be free to engage in intellectual debate without fear of censorship or retaliation.[1] The concept allows faculty and students the right to express views in an open manner. However, this concept is often invoked by faculty when they are concerned that policies and controls that the university or AMC wants to implement will constrain them, even if it is not something that limits their ability to engage in a free and open intellectual discussion. Academic freedom does not permit a faculty member to "ignore college or university regulations," but it certainly allows them a way to express their disagreement with such regulations.[2]

Academic freedom may be something that faculty members attempt to invoke if they are unhappy with an organization's implementation of any of the solutions discussed above. So, making sure everyone understands what the policy and solutions are designed to protect and not protect is important for an organization trying to ensure good data protection practices. Such good practices should not be implemented in a manner that would impinge on academic freedom.

The Family Educational Rights and Privacy Act

Another area of concern for AMCs is the data of students under the Family Educational Rights and Privacy Act (FERPA). The way this data is maintained can also create risks. If employees and faculty are keeping this type of data on mobile devices, there could be issues for the organization if the data is not properly secured.

Although there is no specific regulatory obligation to notify students of a breach of their data, similar to that under HIPAA, the Federal Department of Education (DOE) has taken the position that universities who receive Title IV federal student aid (FSA) funding must notify students of a breach or suspected breach of any data, not just FSA data. The authority for this position has yet to be played out. DOE has stated this is a requirement under the Student Aid Internet Gateway (SAIG) Agreement signed by the institution.[3] This is certainly another area for AMCs to keep their eyes on. DOE has threatened fines for non-compliance and indicated it could withdraw Title IV funding if the college or university cannot demonstrate a robust security program.[4]

Conclusion

The challenges and cost of trying to protect sensitive data will only continue to increase in AMCs, so an AMC must assess its risk tolerance. The risk to PHI carries regulatory sanctions if it is not properly protected. The risk of not properly protecting other types of sensitive data that may not be PHI may also carry regulatory risks. For example, individually identifiable information is not always considered PHI. It depends on how it was collected and the organizational structure of the entity holding it. If it is PHI, it too is protected by HIPAA. If the sensitive, individually identifiable data maintained about research subjects is not PHI, there may still be state laws protecting it. The same may be true for individually identifiable information maintained about employees.

All healthcare entities have challenges when ensuring sensitive data on mobile devices is secure. However, the unique and varied structure of an AMC creates additional challenges in that environment. Not only must they contend with HIPAA regulations, but they also must consider FERPA data. They must also ensure that any solutions used to help secure information meet the technical demands of the environment as well as ensuring that the solution does not infringe on concepts such as academic freedom. This is a daunting, but not impossible, task. It takes coordination among the business units if the AMC is a single legal entity and among the different legal entities if there is more than one.

The obligations to protect sensitive information are likely to increase rather than decrease over time. Being prepared to meet those challenges through a strong information privacy and security program continues to be one of the best defenses. CT

Endnotes

[1] Cawry Nelson, "Defining Academic Freedom," *Inside Higher Ed*, December 21, 2010. https://bit.ly/2cG1ak9

[2] Ibid.

[3] U.S. Department of Education, Federal Student Aid Office: Frequently Asked Questions about Cybersecurity Compliance. https://bit.ly/2EXsOXF

[4] Ibid.

- Information security and privacy challenges are present in all healthcare organizations.
- Academic medical centers (AMCs) may have additional challenges not present in other healthcare organizations.
- Understanding what academic freedom is, versus what it is not, is key.
- There are regulatory enforcement agencies beyond OCR to consider.
- Coordinating efforts between multiple parties will increase the success of the AMC's information privacy and security program.