

Information Security in Healthcare



*Kevin Doyle, CISSP,
ISSMP, CISM*

Security Audit and
Assessment
Manager

Four Critical Errors

As the first Information Security Manager at a fairly large financial institution, I lived by trial and error for a while. Admittedly, I made mistakes along the way, but the good thing is I learned from them and most of the time put what I learned to use.

Working with managers at various types of organizations, such as health care providers, has also been a learning experience. I have learned that we are all human and are prone to seeing and reacting to new laws, major incidents, trends, etc. However, that is what I refer to as *reactive* Information Security Management. Realistically, that is the biggest problem with how information security has been deployed since we were charged with this task. It is how the vendors deploy solutions, and it is how senior management communicates concerns to information security management. “This solution will help you to address the latest phishing threats.” “How are we making sure that the congressman’s medical condition won’t show up in the newspapers, like it did at the hospital on the other side of town?”

The errors below are some critical mistakes that are made when dealing with information security in health care institutions. All of them are either directly or indirectly related to being *reactive* rather than having a *proactive* Information Security Risk Management program in place. After all, Information Security is about defining the critical information generated, assessing the risks to that information, and mitigating the risks by implementing controls and solutions that are consistent with the mission and objectives of the organization.

Information Security in Healthcare (cont.)

By Kevin Doyle, CISSP, ISSMP, CISM

1) Presuming that HIPAA Compliance is Security –

Legislators are concerned about their constituents, because that is who elects them. HIPAA was enacted as a reaction to security breached of healthcare information about consumers. It is important to protect private healthcare information. Privacy is a major concern of security, but it is not the only concern.

Healthcare providers have created positions for Privacy Officers, strictly to comply with HIPAA. Some of those same organizations don't even have a full time Information Security Officer. The three major concerns of information security are the confidentiality, integrity, and availability of information. Privacy is a part of confidentiality. The most critical security concern of health care organizations is the integrity and availability of information, rather than the privacy. Doctors and nurses require accurate information at all times to provide adequate care for patients.

By deploying disproportionate resources to protect privacy as opposed to the other security concerns, we are ineffectively managing resources.

2) Basing Security on the Systems Rather than the Critical Information–

This mistake is one that I made initially when managing my security program. I developed policies but was ineffective at

Information Security in Healthcare (cont.)

By Kevin Doyle, CISSP, ISSMP, CISM

educating users. I spent a lot of money on protecting my systems. Firewalls, intrusion detection systems, filtering solutions, etc. were put into place. In the meantime, users with access to all of that information could easily walk out the door with paper reports full of critical information and I never would have known it unless a problem occurred. But I had the toys to protect my *technology!*

Security must be looked at holistically. Information is in all forms, not just on the systems. Information Security must assess the risks to information in all forms and in how it is transmitted from one party to another. Ignoring that principal results in many breaches that occur.

3) Ineffective Awareness Programs—

Another lesson that I learned is that users care about security, but only if it does not interfere with what they have to get done. The key in that statement is that they **DO** care about security. The users' main concern, whether it is the person entering information in the waiting room, nurses, lab workers, or physicians and administrators, is that information and systems are available to do their jobs.

Very few people *want* to disclose private information to the wrong parties, or intentionally enter inaccurate information about patients into a system. They recognize that security is important. However, ineffective awareness programs do not create the culture needed to protect information at the human level.

Information Security in Healthcare (cont.)

By Kevin Doyle, CISSP, ISSMP,
CISM

Information security awareness is about teaching people to be part of a team to protect information. There are ineffective and effective ways to accomplish this. Effective programs will result in users being alert to parties trying to get information or access they are not entitled to. These programs are not viewed as a nuisance, but as a persistent tool that can help users effectively perform their job.

Without an effective program, accidental security breaches are likely to occur.

4) Failure to Control Access to Information—

One of the trickiest parts of managing security is one of its most basic principals. Users should have access to sensitive information on a “need to know” basis.

The two main inhibitors of applying this principal is (1) failure to define what sensitive information is; and (2) failure to remove or modify access when employees leave their job and either take another position or no longer work for the organization.

Without defining what information and systems are sensitive, we tend to over-protect or under-protect information. This either results in wasted money or breaches. Neither is a desired result. The first step in protecting information is to classify what should be protected.

Information Security in Healthcare (cont.)

By Kevin Doyle, CISSP, ISSMP,
CISM

We also fall to the demands of “give me the access I need to do my job NOW!” We react to the demand, and don’t remove the access the user had that they no longer need. Complicating it is the multitude of applications, both client-server and web-based, required by users.

To effectively manage employee transitions and terminations requires a team effort between the user departments, Human Resources, Information Technology and Information Security. Not getting a handle on this can create quite a mess that is difficult to clean up.

Summary–

The errors above are not the only errors we can make, but they are some of the most glaring and costly mistakes that are made that lead to ineffective security and breaches.

A proactive, holistic approach to information security based on risk management of the most critical information in an organization will protect not only the confidentiality and privacy of information, but its availability and accuracy as well.