

Diagnosing “Sanctionable” Offenses Through Technology

There are countless pieces of technology that have helped advance the healthcare industry to where it is today, and few would dispute that the computer is at the top of this list. No other device is as heavily and universally relied upon throughout healthcare as this wonderfully complex manipulator of binary code. After all, computers add efficiency and capability in every room – from the waiting room to the boardroom and from the ER to the OR. But as the saying goes, “With great power comes great responsibility.”

To this end, healthcare organizations have been strapped with the task of meeting compliance with HIPAA. This venerable piece of legislation lies out in no uncertain terms that healthcare providers must do whatever is reasonable to protect the integrity and privacy of patient data. As the industry becomes more dependent upon computers to manipulate and maintain patient information, proper care must be taken to ensure that said data is not corrupted or placed in the wrong hands. Possibilities of such corruption or information “leakage” are multiplied exponentially by the addition of an Internet connection to the computer network.

Of course, the first step in any good HIPAA compliancy plan is to formulate a set of procedures or guidelines, that when properly followed will assure the integrity and privacy of patient data. Once the staff has been thoroughly educated on these procedures, the next step is to put in place a reasonable yet strict policy for sanctioning those who may violate the rules. When speaking of computers and Internet usage, there are many items that could (and in most cases should) be noted as sanctionable offenses. Some common items that should certainly be addressed include:

- Weak passwords or shared passwords
- Accessing “prohibited” files (confidential or not relevant to your work)
- Theft or unauthorized copying of any company data for personal use
- Sending e-mail that contains PHI
- Improper or non-productive usage of the computer network or the Internet
- Unauthorized installation of any program

The above list highlights some of the most flagrant violations of network usage. The commonality amongst every item on this list, however, is that most organizations (healthcare or otherwise) do not know when these violations are occurring. And it is very difficult to sanction someone for an offense if that offense sneaks “under the radar.”

Thankfully, there exists a multitude of technologies to assist healthcare organizations in their quest for HIPAA compliance. For the most part, these technologies take one of two types of action – logging or blocking. To have the best security posture, it is our belief that the question to be addressed with every “addressable item” is not IF an action should be taken, but WHICH action – logging or blocking – should be taken. There is simply no excuse for having a poor or inadequate security posture when it comes to HIPAA compliancy, especially considering the number of simple and cost-effective tools that exist in the marketplace today.

For example, password management is one of the easiest technologies to deploy but one of the most commonly overlooked. A good password management software will enforce company-designated password requirements (minimum number and type of characters), as well as a periodic changing of passwords. With these solutions, network administrators can either log creation of insufficient passwords or block their use altogether.

Many organizations today are even combining password management software with single-sign-on technology to make their workers more efficient while improving their security. To prevent password sharing, an institution can also bundle multi-factor authentication into the mix, combining something a user knows (their password) with something they have (an access card or even a thumbprint). In this scenario, User B would be blocked (and logged) from accessing User A's account without both the password and access control device.

Similar tactics can be used with any of a large number of potential security violations. Intrusion detection/prevention software can log or block the installation of programs or the usage of peer-to-peer file sharing applications, etc. Content filters can log or block unproductive and potentially offensive Internet usage. Accessing prohibited files and/or copying them to media devices (such as CDs or USB drives) can also be logged or blocked. And e-mail that contains PHI can be logged, blocked, or even encrypted and sent on.

The point here (as shown by all of the clever underlining) is that virtually any potential threat to your organization's data can be dealt with in one of two ways. You may choose to simply log violations in order to have private conferences with those employees who may present a problem through repeated offenses. Or you may choose to run a tighter ship and block all malicious activity before it happens. You may choose any combination of the two courses of action that best meet your company's needs and objectives. What you absolutely should not do is make the choice to ignore these items.



FORTRESS Network Security provides a number of products and services that Covered Entities can use to ensure their compliance with HIPAA while using computer resources. These solutions meet the Security Rule requirements, and include other features that support HIPAA compliance by Covered Entities. If you would like more information on said products or services that will assist you in your goals of logging/blocking inappropriate computer usage, please contact us toll-free at 866.948.7377 and/or visit our website at <http://www.fortressnetworksecurity.com>