Intrusion Prevention Systems

In the Healthcare Environment

Lakisha Thomas

ICTN 4040
Healthcare organizations are in the midst of a complete turn around in regard to information security and privacy. Years ago a health care facility was viewed as an “open environment.” With hospital networks interconnected with Universities, clinics and other hospitals, the demand for security is implemented but not really enforced at times. With this “open environment” medical students could browse through medical records with ease. Hackers could get into the system and prevent authorized users from obtaining medical records. Today those security issues have changed. Healthcare facilities are becoming more secure and accountable for patient information and access to it. The primary reason for healthcare facilities to insure security and privacy of patient information is because of the Health Insurance Portability Act (HIPAA) of 1996.

Congress enacted this act with a focus on healthcare reform. HIPPA is aimed to improve the efficiency of healthcare data and processing through the standardization of administrative and financial data transactions, while protecting the privacy and integrity of patient information. The HIPPA regulation includes specific sections on privacy and security. The privacy standards require the protection of patient data from inappropriate and unauthorized disclosure or use. (3) The security standards require the safeguarding of patient data from unauthorized access. The securities fall into three categories: Administrative, Physical and Technical Safeguards. Administrative safeguards administer actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information. Physical safeguards measures policies and procedures to protect a covered entity’s electronic information systems and related
buildings and equipment from unauthorized intrusion. Technical safeguards protect health information and control access to it. (1) Figure 1 is just an overview of the healthcare security trends that are implemented in healthcare organizations.

![Healthcare Security Trends](image)

**Figure 1**

Healthcare organizations are challenged to make information more available to physicians and patients. Patients want to access their medical data online. Physicians want immediate access to lab reports and diagnosis – at times remotely. More and more medical devices are also being connected to large healthcare networks, often with exposed commercial operating systems. Today healthcare providers are using high tech security methods in compliance with the HIPAA Act. Providers are using biometrics, smart cards, RFIDs and other IPS hardware and software components. Most hospitals, government health agencies and other facilities are using intrusion prevention systems (IPS) to secure patient information. Intrusion prevention systems were invented independently by Jed Haile and Vern Paxon. IPSs are considered “the next level of security technology with its capability to provide security at all system levels, from the
operating system kernel to network data packets.” (6) Along with an IDS, it provides policies and rules for network traffic and sends an alert when a hint of suspicious traffic has tried to enter. IPS makes an attempt to stop any potential attack. I see IPS as a better version of IDS and firewall protection at the application layer. ISP is similar to IDS because it has two types of intrusion prevention systems, host-based and network-based. Host-based intrusion prevention systems (HIPS) are used to protect both servers and workstations through software. HIPS catches suspicious activity on the system and then notifies the system or blocks the attack from happening. It monitors application or data request, network connection attempts and read and write attempts. A network-based intrusion prevention system (NIPS) intercept all network traffic and monitors it for suspicious activities and events. It usually scans for intrusion signatures, searches for protocol anomalies, detect commands not normally executed on the network and more. If the system finds an offending packet of information, it can rewrite the packet so the hack attempt will fail. When this happens, the organization can take this information and use it as future references when something like this happens again. They would know what to expect and how to handle the situation in a timely manner. The main disadvantage to intrusion prevention systems is the cost. The cost to install the software to each and every server and workstation within the organization may be very expensive. The HIPS on each system must also be updated frequently to ensure attack signatures are up-to-date. Some network request that may be legitimate may also be blocked which would cause the network performance to drop. To be effective, an Intrusion Prevention system must also be a very good Intrusion Detection system to enable a low rate of false positives.
With all the security features out today and the HIPAA Act in place, health care facilities feel that they need to improve their security of information by installing an IPS. According to Bonnie Norman, system security engineer for Wellstar Health System, “The main reason they wanted to use some form of IPS is because of what they learned in the SANS Hacker Tools and Incident Handling Class. It showed us the tools the hackers are using and how they get around the standard defenses that we and other organizations were using.” Wellstar Health System used the IPS TippingPoint. TippingPoint’s intrusion prevention systems are designed to meet the growing demands of increased availability, comprehensive security and regulatory compliance of healthcare organizations. TippingPoint meets HIPAA requirements for securing health information. TippingPoint’s IPS protect against unauthorized access to the network and malicious attacks against network equipment and medical systems. It provides constant vigilance against emerging vulnerabilities. It also provides detailed reporting options for reviewing network behavior blocked attacks. TippingPoint also stops spyware from being installed. It also blocks outgoing traffic attempting to reach the spyware data collection sites. In a health care environment computer viruses can cause tremendous problems when trying to retrieve medical records. The TippingPoint IPS enforces security by preventing unauthorized access to PHI at the network layer. The system detects and prevents viruses and worms from gaining access to the network. All attempts to access the network are verified and mitigated if considered malicious or false. The Threat Suppression Engine scans and blocks access and potential threats in network traffic. Without some form of security hackers can get into the system and obtain patient information. If a worm, virus, or denial-of-service attack occurs, doctors are unable to
access electronic patient records or digital images which can compromise patient care. It could also hinder administration from filing insurance claims. Universities that are connected with medical centers are more vulnerable to malicious activities. Thanks to this technology medical centers can protect their information from getting into the wrong hands of student users and other potential hackers. Figure 2 shows an example of ISPs implemented at a Hospital/Healthcare Provider.

Figure 2

When Hurricane Katrina hit the Gulf Coast, government health agencies would be handing a nearly unprecedented volume of new, temporary networks, systems and shelters. Those networks would serve as a major communications link between hurricane survivors and their families and friends, as well as between the numerous shelters and the main office. Ensuring the confidentiality and availability of the information traveling through these networks would prompt healthcare organizations to implement ISPs in their network. Without the use of high-tech security methods patient’s information is left out
for everyone to view and take advantage of. It’s a problem now with victims trying to regain their identity and trying to get things back to normal. The last thing they want to worry about is someone obtaining their medical information and maybe altering it. This could affect the patient in many ways. Someone could tamper with their medical records and put things that may not be true which could affect the patient in the long run. They could be prescribed a medication that they may be allergic to, but the record doesn’t say anything about this. I think that it’s a very important issue to all people, but especially to Katrina victims. The question would be, “Will health organizations in the Gulf Coast be fined if medical records were disclosed to the public?” Would this be a special circumstance and if something tragic like this happened again would the government continue to let things “slide” because of what happened? People’s information is still being let out in the open regardless of the situation. If the American Red Cross can implement IPSes than there is no reason for healthcare environments to not place IPSes in their network.

In conclusion, personal information is just that, personal. No one wants their medical records to be published or tampered with. It’s up to the healthcare industry to make sure this doesn’t happen. Individuals trust this industry to keep all confidential information inside their environment and would hope that no one can obtain such information. It’s up to the healthcare organizations to make sure no one tampers with their network. If companies can’t keep up their end of the bargain then they should be fined according to the HIPAA Act. I think this was a great idea to put into legislation. Patient confidentiality is just as important as social security numbers and any other personal information and should never have a chance to be released. Healthcare
organizations should go above and beyond the call to make sure they have the latest technology and security features. They have a lot at stake to just ignore upgrades or ignore including Intrusion Detection or Intrusion Prevention Systems in their networks. Hackers are always finding new ways to get around certain networks. It’s the security’s department primary goal to stay on top of new viruses, worms and malicious attacks and to make sure their organization is prepared for these attacks and how to respond to them.
References

1. Securing Critical Data and IT Infrastructure in Healthcare Environments Artical
www.tippingpoint.com

Health Data Management, September


5. Martin, Zach, “Username and Passwords Still Reign in Health Care,” IDNewswire,
Vol. 4 No. 2 January 28, 2005

6. www.webopedia.com