Joint Security and Privacy Committee

International Medical Informatics

www.nema.org/medical/spc

Secretariat: NEMA (National Electrical Manufacturers Association)
1300 North 17th Street, Suite 1847, Rosslyn, VA 22209 USA
tel: +01-703-841-3200 fax: +01-703-841-5900
Chairman-NEMA: John Moehrke, GE Healthcare, john.moehrke@med.ge.com
Vice Chairman-JIRA: Hitoshi Yoshimura, KonicaMinolta, yoshimura.h@konicaminolta.jp
Vice Chairman-COCIR: Wolfgang Leetz, Siemens Medical Solutions, Wolfgang.Leetz@siemens.com
Secretary: Stephen Vastagh, NEMA, ste_vastagh@nema.org

To: National Committee on Vital and Health Statistics (NCVHS)
Subcommittee on Privacy and Confidentiality

From: The Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC)
Stephen Vastagh, Secretary (703-841-3281) for James Keese and Peggy Hanney, testifying on behalf of the SPC to the Subcommittee on Privacy and Confidentiality

Date: December 2, 2004

By e-mail to: mrawlinson@cdc.gov
Cc: AChapper@cms.hhs.gov

Re: Impact of the HIPAA Security Rule regulations on medical device security

This submission is in response to the Subcommittee Chairman's invitation and request to submit additional information and recommendations to the Subcommittee within two weeks of the testimony on Nov. 19, 2004. These recommendations represent a practicable and sustainable approach to medical device-related compliance. They were developed by the SPC in consultation with the Department of Veterans Affairs Veterans Health Administration (VA/VHA) and with the US Army Medical Research Material Command (MRMC).

Recommendation

With regard to the HIPAA Security Rule, we recommend (1) an immediate education action by the government, and (2) an adjustment to the enforcement of the HIPAA Security Rule to use Phased Enforcement:

Immediate education action: FDA to establish a single issue message on its website similar to www.fda.gov/cdrh/ct . This forum can be used to quell some of misquotes and misunderstandings. For example:

a. Healthcare providers need to work with their vendors, but if that doesn't work they have the option to use the MDR mechanism.

b. Cybersecurity hazards need to be treated using the same SOP as any other hazard.

c. Use of automatic patch application without proper validation is irresponsible and could cause patient harm.

Phased Enforcement:

Year 1: All covered entities must complete Risk Management Planning on all devices that contain ePHI. Risk management planning should address patient safety, medical effectiveness, privacy, and security. This concludes with an enterprise-wide, clear, demonstrable prioritized list of planned mitigations with the highest risk devices having mitigation implementation underway and the lower-risk threats being planned for external control or device replacement rolled into the next procurement cycle. (See discussion below)

Year 2: Demonstrated completion of first-round mitigations and the establishment of subsequent targets. Demonstration of HIPAA-driven procurement specifications and completed processes for sustainable risk management.

Year 3: Demonstrated progress in meeting or exceeding HIPAA security targets. Implementation of first-round medical device security process audits confirming both processes and verifying selected device security.

Year 4+: Continuing evidence of device compliance growth and sustainability of security programs.

By creating a known enforcement policy and supporting this with educational materials for the approximately 5,900 non-governmental hospitals in the Unites States, the DHHS can meet its goal of securing protected health information in a way that is sustainable and one that insures the continuity of care for those who rely on the US healthcare community.

RATIONALE, SUPPORTING INFORMATION

Information technology (IT) security relies on achieving Confidentiality of information, Integrity of information, and Availability of information (referred to as C-I-A). Adequate security can be defined as the best C-I-A balance while still supporting the primary mission of the enterprise. In healthcare, the care delivery organization strives for maximum quality and continuity of patient care while maintaining the proper balance of C-I-A. The HIPAA Security Rule directly addresses confidentiality in IT systems that manage electronic protected health information (ePHI). We believe that the Security Rule provides enough latitude for achieving appropriate levels of integrity and availability necessary to carry out the mission. However, it is clear that there is confusion in the provider community about applying these rules directly and immediately to medical devices.

This paper suggests that more explicit guidance be provided by DHHS in achieving the long-term security goals for medical devices and the healthcare systems that rely on them.

Issues: HIPAA Security Rule and medical devices

1. The language used in HIPAA regulations and those used in FDA regulations often differ.
2. The goals of FDA regulations differ from HIPAA regulations. The FDA quality system regulation priorities focus on (a) safety to patient and operator and (b) effectiveness in carrying out the healthcare mission. To this, HIPAA adds (c) privacy of information.
3. There is a threat to healthcare due to:
    a. The use of commercial off-the-shelf (COTS) hardware and software platforms in medical devices.
    b. Increases in security exploits against COTS software.
    c. A rise in the frequency of recommended critical patches to COTS software by 3rd party software vendors.
4. There exists a formidable gap between the three to seven year medical device development cycle and the new security requirements (6 to 24 month-old).
5. Medical devices typically have lifetimes from five to twenty years. Typical security support for COTS operating systems is three to five years.
6. Most healthcare organizations are at a low level of security recognition in (1) understanding and specifying medical device features and (2) in the management of medical device security in healthcare organizations. Some healthcare provider IT organizations are beginning to exert control over the management of medical devices.
7. Continuing healthcare cost containment over the past five years has resulted in (1) improved IT/connectivity-reliant workflows, (2) reduced IT staff and (3) hospital-wide, simplified (flattened) networks.

Risk Management Planning

The way to address the above points while addressing Security is for the Healthcare Providers to follow the Risk Management process required by the HIPAA Security rule. We propose that DHHS require the use of risk management as part of the enforcement of HIPAA.[1]

Risk Management Methods

The basic steps in Risk Management are:

1. identification of assets, access, actors, and motives in the elaboration of threats to ePHI for the medical device in its operational environment.[2]
2. the explicit scoring of risk as the product of likelihood of exploit and severity of exploit. Here severity judgments would include adherence to HIPAA required and addressable elements.
3. consideration of proposed mitigations to the threats (which may include the device manufacturer-supplied technical security features and/or external means of

securing a device.) The mitigations used must be evaluated to ensure that they do not compromise patient safety or medical effectiveness.

4. re-scoring the threats after proposed first-round mitigations and elaborating the prioritized residual risk so hospital management can make appropriate risk-based decisions on mitigation versus replacement.
5. regular and sustainable re-execution of steps 1-4 above surfacing new threats and verifying the mitigation of previous threats.
6. auditing the entire risk management process to assure quality performance and improvement through risk-reducing targets.

Risk management is done in a covered entity's organization through local medical device risk assessment conducted by multidisciplinary teams that are able to plan and execute the above steps while recommending resource investment to hospital management. Medical device manufacturers supply the team with information on device security features (for example the MDS^2 form developed by HIMSS[3], Service Manuals, Operator Manuals). The risk management team creates a risk summary document that serves as a basis for risk-based decisions by hospital management.

To get through the transition, we have proposed that DHHS take a *phased enforcement* approach to the securing of ePHI. While this *phased enforcement* is underway, providers and manufacturers will continue to work together in organizations like HIMSS[3], NEMA/COCIR/JIRA SPC[4], and others to improve security of ePHI. At the same time, DHHS and FDA need to support education outreach to all healthcare organizations to help them in achieving security maturity.

References

[1] Austin R.D. and Darby C.A.R. 2003. The Myth of Secure Computing. Harvard Business Review. June 2003.

[2] Alberts C. and Dorofee A. 2002. Managing Information Security Risks: The OCTAVE Approach. 471 pages. Carnegie-Mellon Software Engineering Institute. Addison-Wesley, Boston MA.

[3] HIMSS Medical Device Security Workgroup. 2004. Manufacturer Disclosure Statement for Medical Device Security. http://www.himss.org/asp/medicalDeviceSecurity.asp

[4] Joint NEMA/COCIR/JIRA Security and Privacy Committee. http://www.nema.org/medical/spc