CYBER SECURITY
INDUSTRY ALLIANCE

Ten Steps for Securing Electronic Health Care Systems

April 2005

Ten Steps for Securing Electronic Health Care Systems

CYBER SECURITY INDUSTRY ALLIANCE

APRIL 2005

The Cyber Security Industry Alliance (CSIA) welcomes President Bush's initiative to provide all Americans access to electronic health records within the next ten years. Technology enabling this access will also improve the quality of health care, save billions of dollars for providers and reduce the cost of health care for all Americans. Hospitals using electronic prescription systems have already cut prescription errors by up to 80 percent. Quality-of-care measurement systems used by Medicare in hundreds of hospitals are showing improvements of about six percent. The Department of Health and Human Services (HHS) conservatively estimates savings from technology will reach $140 billion a year by 2014 – about six percent of health care spending in that year. Health care accounts for about 15 percent of the U.S. economy so these gains will have significant impact on the overall economy.

Cyber security is a major priority for enabling electronic health care systems. Personally identifiable health care information must be protected from all unauthorized access, whether it be from deliberate attacks by external hackers, by disgruntled employees, or even from simple procedural oversight. Equally important is the integrity of health records – they must be assured and available immediately for urgent medical procedures. A broad range of technical solutions are available now for establishing and ensuring strong cyber security by health care organizations. In support of the Administration's efforts, the CSIA offers the following "Ten Steps for Securing Electronic Health Care Systems."

BACKGROUND

The creation of a secure, centralized electronic medical record is a clear priority for the U.S. Department of Health and Human Services (HHS). According to a HHS Fact Sheet:

> *HHS is working aggressively to promote the use of technology to improve patient safety and to allow quick, reliable and secure access to information that promotes the best possible care across the health care system. A key part of this broad effort is developing a National Health Information Infrastructure -- a system that would allow a doctor or other health care provider to access an always-up-to-date electronic health record for a patient who has authorized it, regardless of when and where the patient receives care. This would not be a national database, but rather a set of standards and secure networks that would allow a doctor or hospital to immediately gather relevant information by computer network.*

The information would be protected by stringent security and privacy standards. Such a system would also help consumers and patients to manage their own health by giving them greater control of their health records.

President Bush ordered the creation of a central office at HHS to oversee this complex effort and appointed Dr. David Brailer as coordinator. The National Health Information Technology Coordinator was directed to report to and assist the Secretary on privacy and security issues related to the development of a national health information infrastructure and to recommend methods to assure appropriate authorization, authentication and encryption of data to protect the privacy and confidentiality of personal health information. CSIA has recommended that the National Coordinator use the following "Ten Steps for Securing Electronic Health Care Systems" to help foster development of a more secure healthcare information infrastructure.

TEN STEPS TO SECURING HEALTH INFORMATION SYSTEMS

Health care information systems carry information that goes beyond the typical definitions of "mission critical" and into issues that can affect life and death. Cyber security demands special attention in this environment.

The health care information infrastructure includes: hospitals, doctor's offices and medical clinics, nursing homes, laboratories, insurance companies, and, of course, patients. When building the electronic health care information system, think about security from the start. Delayed consideration is costly and will affect patients' and medical practitioners' trust of the network.

Information security begins with the tone of policy at the top. The National Coordinator, senior executives and boards of directors of health care-related industries should conduct regular reviews of the status of their cyber security programs.

"C.I.A." Information Assurance Strategy

- **Confidentiality** – protection from unauthorized access or disclosure (1-3)
- **Integrity** – protecting information from unauthorized changes (4-6)
- **Availability** – redundancy and protection for critical systems (7-10)

CSIA recommends use of the following ten steps to help secure electronic healthcare systems.

1 Deploy strong authentication and authorization controls. These technologies answer the basic questions: "who are you" and "what can you do?" The use of such controls—which include secure ID tokens and digital certificates—will ensure only authorized users gain access to a system and to only those parts of the system necessary to perform his or her responsibilities. Passwords are not enough. They are easily defeated or compromised enabling an attacker to assume another's identity. Appropriate authentication and access controls protect against not only unauthorized access, but also reduce the risk of systems being infected by malicious software (malware) spread via Trojans and worms.

2 Encrypt data and communications when appropriate. Data residing on hard drives, hand-held computers, or other storage devices must be protected by

strong cryptographic technologies such as the Advanced Encryption Standard (AES) developed by the US National Institute of Standards and Technology (NIST). Likewise, health care data in transit must be protected from unauthorized interception or eavesdropping. The challenge will be providing strong cryptographic technologies end-to-end, where end points will range from patient's homes to large hospitals, and often may terminate in a mobile device such as a personal digital assistant (PDA) or Internet-enabled cellular telephone. Fortunately, security solutions already exist that allow users to seamlessly encrypt e-mail and databases.

3 Properly dispose retired equipment and data. As data is modified, updated, or corrected, old data must be purged in a manner that prevents unauthorized users to access or recover the information. This includes proper disposal and destruction of mass storage devices, physical outputs of printers or other peripheral devices, and other locations where old information might be recovered by unauthorized users. Certified data destruction technologies that will meet this requirement are available from multiple commercial sources.

4 Validate data. More and more data is being entered into systems via the web given the need for a simple, interoperable, and easily accessible interface. Web-based user interfaces should be used to support a modern health care information infrastructure, but they are vulnerable, potentially enabling an attacker to change or manipulate data. However, solutions are available to ensure the security of websites as well as the databases linked to those websites.

5 Conduct frequent system audits. While security measures should be deployed across the information systems, all transactions must be audited to ensure only those authorized to use the system are accessing, entering, or changing information.

6 Use digital signatures and secure date-time stamps. Use cryptographic checksums, fingerprints, or signatures to verify that data whether in transit or in a database has not been modified by unauthorized parties. Digital signatures ensure that the accompanying data is tamperproof and that signers cannot later deny access or use. Secure date-time stamping documents exactly when a record was created or modified.

7 Provide for redundancy. As with all large data storage and retrieval systems, there will be occasions when parts of the electronic health care records system will be unavailable due to equipment failure, denial of service attacks, or scheduled down time. Redundancy in the system at the data entry, storage, and retrieval levels will reduce or eliminate most availability problems.

8 Use a private data backbone. Network bottlenecks and outages are a continuous Internet problem due to fluctuations in data flows and the reliability and performance of various portions of the Internet. Even though access to major portions of the system by patients and health care professionals will be via the Internet, the backbone network of this system must be carried via a private data network in a manner similar to those used by banks and financial institutions.

9 Develop a rapid incident response mechanism. Attacks, intrusions, and events affecting the security of the healthcare records system will occur. Frequently these incidents result in unnecessary down times and delays while the investigators retrieve information and forensics data from the impacted systems. To avoid or shorten these periods of unavailability, a robust and rapid incident response mechanism should be integrated into the initial design of the system, and given high priority for action. Establish a crisis management team which includes senior-level representatives who can convene and act quickly. Assign roles and responsibilities for each member of the team and exercise your plans regularly.

10 Sponsor information sharing networks. Rapid and trustworthy information sharing between system administrators, security professionals, and senior managers is a key component of a well designed information security plan. In recent years, Information Sharing and Analysis Centers (ISACs) have been established in all of the critical infrastructure sectors including the banking and finance, transportation, energy, and telecommunications sectors. While there have been efforts to stand up Health Care ISAC, Federal support would make it much stronger and more effective. The Departments of Treasury, Energy, Homeland Security, and Transportation provide financial support to their respective ISACs. HHS should examine these models and lend appropriate support to the Health Care ISAC. HHS support and promotion of ISAC membership among hospitals, medical clinics, laboratories, and insurance companies would greatly assist in the timely dissemination of cyber threats, vulnerabilities, and attacks.

ABOUT THE CYBER SECURITY INDUSTRY ALLIANCE

The Cyber Security Industry Alliance is an advocacy group to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. Launched in February 2004, the CSIA is the only public policy and advocacy group comprised exclusively of security software, hardware and service vendors that is addressing key cyber security issues. Members include BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc., Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc., iPass, Inc., Juniper Networks, Inc., McAfee, Inc., PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation, Symantec Corporation, and TechGuard Security.

Cyber Security Industry Alliance
2020 North 14th Street
Suite 750
Arlington, VA 22201
(202) 204-0838
www.csialliance.org