CYBER SECURITY
INDUSTRY ALLIANCE

Response to Consultation Community Action on Health Services

Ten steps to building a secure electronic healthcare system

31 January 2007

Introduction

The Cyber Security Industry Alliance welcomes this opportunity to participate in the Commission's Consultation regarding Community action on health services. Our comments are focused on the need to ensure the safe and secure sharing of health-related data across Europe an issue referred to on two different occasions in the document (page 6 and 7).

Ten Steps to Building a Secure Electronic Health Care System

Health care information systems carry information that goes beyond the typical definitions of 'mission critical' and into issues that are 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 an electronic health care information system, one needs to think about security from the start. Delayed consideration is costly and will affect patients' and medical practitioners' trust of the network.

Information assurance is often broken into three principle areas of focus: confidentiality, integrity, and availability. Each is useful in developing a comprehensive information security strategy and can be applied to the challenge of creating a secure electronic healthcare system.

Confidentiality – Protect Patient Information from Unauthorized Access or Disclosure

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.

At the same time, evidence shows that issues most often stem from inside an organisation, with authorised sources taking actions that are inappropriate, sometimes deliberately, sometimes in error, resulting in unauthorised access to confidential data by third parties. Activity monitoring on critical databases is therefore essential to be able to identify and rectify issues as soon as they emerge.

2. Encrypt data and communications wherever 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. Destroy expired data. As data is modified, updated, or corrected, old data must be destroyed 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.

Integrity – Protect Patient Information from Unauthorized Changes

4. Validate data. More and more data are 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. 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 provide the additional security aspect of non-repudiation.

Availability – Ensure Redundancy and Protection for Critical Information Systems

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.

About CSIA[1]

CSIA is an advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Launched in February 2004, its members include the leading cyber security software, hardware, and service companies. The organisation is led by CEOs from the world's top security providers, all international companies with a strong European presence. Its members include:

APPLICATION SECURITY, INC.
BSi
CiTRIX
ca
CROSSROADS Assuring Global Information
Entrust Securing Digital Identities & Information
FORTINET
F-SECURE
IBM
iPass
McAfee
mirage networks
MXI SECURITY
PGP
QUALYS
RSA The Security Division of EMC
SECURE COMPUTING
SURETY
SurfControl
symantec.
TECHGUARD SECURITY
VONTU

For further information, please contact

Liz Gasster
Acting Executive Director, CSIA
2020 North 14th Street
Suite 750
Arlington, VA 22201
USA
Tel +1 (703) 894 1263
lgasster@csialliance.org

Marika Konings
Director of European Affairs, CSIA
Rond Point Schuman 6, box 5
1040, Brussels
Belgium
Tel +32 234 7850
mkonings@csialliance.org

[1] www.csialliance.org

This paper represents the views of its author on the subject. These views have not been adopted or in any way approved by the Commission and should not be relied upon as a statement of the Commission's or Health & Consumer Protection DG's views. The European Commission does not guarantee the accuracy of the data included in this paper, nor does it accept responsibility for any use made thereof.