White Paper

Meeting HIPAA Requirements with Federal Information Process Standard (FIPS) Encryption

Today's healthcare IT industry is being transformed by dramatic changes in patient information management. Government regulation and technology advances have fueled explosive growth in creating and storing protected healthcare information (PHI). Organizations are looking for secure, reliable, and cost-effective technologies to help them comply with the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act governing storage and management of medical information.

Signed into law by President Barack Obama as one of the provisions of the American Recovery and Reinvestment Act of 2009 (ARRA), the HITECH Act stipulates significant penalties against medical organizations for creating a breach of unsecured protected health information (defined as "patient health records that have not been made unusable, unreadable, or indecipherable to unauthorized individuals"). This strengthens the regulations previously outlined in the Health Insurance Portability and Accountability Act (HIPAA), which was signed into law in 1996. HIPAA was the first act to require national standards for electronic healthcare transactions and, among other things, addresses the security and privacy of health data.

To achieve compliance with the HIPAA standard, healthcare providers are increasingly turning to verified, certified network security products and architectures offered by networking leaders such as Cisco. The U.S. Department of Health and Human Services (HHS) recommends products certified for the Federal Information Process Standard (FIPS) 140-2 encryption standard to protect healthcare data. Already mandated by the U.S. Department of Defense (DoD) for encryption, FIPS 140-2 is a powerful security solution that reduces risk without increasing costs.

The HITECH Act offers economic stimulus funding through 2014 to help providers achieve meaningful use of their medical information. This opportunity makes it the perfect time for providers to consider an investment in information security.

The Risks of Noncompliance

The healthcare industry is well prepared for many types of emergencies and problems, according to the 2012 National Preparedness Report conducted by the Federal Emergency Management Agency. However, the same study found that by and large, healthcare providers are not ready to face a cybersecurity attack. According to the report, cybersecurity "was the single core capability where states had made the least amount of overall progress"; only 42 percent of state officials believed that they were adequately prepared.

According to the same report, just under two-thirds of all U.S. companies have sustained cyberattacks over the past six years and, between 2006 and 2010, the number of reported attacks in the U.S. increased by 650 percent. At the Aspen Security Forum in May 2012, the DoD stated that the U.S. has seen a 17-fold increase in attacks against its infrastructure between 2009 and 2011.

In this tumultuous environment, compliance with HIPAA requirements is a top priority. Prior to 2009 and the signing of the HITECH Act, there was a general consensus in the healthcare industry that HIPAA had not been rigorously enforced. Under HITECH, healthcare providers may now be penalized for "willful neglect" if they cannot

demonstrate reasonable compliance with the Act. These penalties can extend up to $250,000, with fines for uncorrected violations of up to $1.5 million.

Under some circumstances, HIPAA's civil and criminal penalties may also now include business associates. While an individual cannot sue a provider, the state attorney general may bring an action on behalf of state residents. As well, the HHS is now required to conduct periodic audits of covered entities and business associates. This means that healthcare providers must have systems in place to monitor business practices and relationships to assure consistent security for all medical information.

In addition to these penalties, providers face significant risks to their business if information systems are accessible to attack. In the healthcare industry, such threats may take a variety of forms:

- The Kern Medical Center in Bakersfield, CA, was attacked by a virus that crippled its computer systems. The hospital took about 10 days to get doctors and nurses back online.
- During an attack on a Chicago hospital, a piece of malware forced the hospital's computers into a botnet controlled by the hacker—and the hospital was still dealing with the consequences of the attack a year later.
- The DoD is facing a multi-billion-dollar lawsuit based on the theft of a computer tape containing unencrypted personal health information from an employee's car.
- The Veterans Administration (VA) waged a two-year war against intrusions into medical device and wireless networks, including picture archiving and communication systems (PACS), glucometers, and pharmacy dispensing cabinets.

Secured management of medical information protects patients against identity theft and discrimination, as well as life-threatening risks of interference with medical equipment or devices. At the same time, information needs to be made available quickly when needed, such as to emergency personnel. The resulting benefits are critical for keeping the business competitive:

- Better quality of care for the patient
- Improved patient outcomes
- Increased productivity and workflow efficiency
- Better information at the point of care
- Improved and integrated communications between doctors and patients

Encryption as the Key to Compliance

To mitigate these risks, service providers are required to assure that information across the healthcare network is inaccessible to an unauthorized user. In April 2009, the HHS issued guidelines recommending encryption using technologies that are compliant with the FIPS 140-2 standard.

According to the Federal Information Processing Standards Publication, FIPS-140 is "applicable to all … agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106."

Cisco's own offering, Next Generation Encryption (NGE), is fully FIPS-140 compliant, providing a security level that will remain compliant even after 2030, unlike older cryptographic systems.

Encryption tools convert the message in a file or document into an unreadable format before being sent, and then decrypt the content at the other end to return it to a readable state. To meet the HITECH Act requirements, encryption must be implemented within both the main service provider network and its associated partner networks. Successful use depends upon the strength of the encryption algorithm and the security of the decryption "key," or process, when data is in motion (moving through a network, including wireless transmission) or at rest (in databases, file systems, or other structured storage methods).

Organizations with completely closed networks that have no outside access may not be required to implement encryption, but they will need to thoroughly document their justification for not doing so. However, closed networks these days are almost nonexistent—any office at least has Internet access. With increased use of electronic transactions in healthcare, including e-prescribing and electronic communication, most medical organizations are using open systems and need to implement encryption tools.

What Is FIPS 140-2?

FIPS 140-2 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. A cryptographic module is the set of hardware, software, and/or firmware that implements approved security functions (including algorithms and key generation) and is contained within the cryptographic boundary. Modules are produced by the private sector or open source communities for use by regulated industries, such as healthcare, that collect, store, transfer, share, and disseminate sensitive information.

The U.S. government requirements for cryptography are documented by the National Institute of Standards and Technology (NIST), a branch of the U.S. Commerce Department. FIPS 140-2, issued on May 25, 2001, is the most current version of the standard. It establishes the Cryptographic Module Validation Program (CMVP) as a joint effort by the NIST and the Communications Security Establishment (CSE) for Canada.

CMVP testing is handled by any one of 13 third-party laboratories accredited as cryptographic module testing laboratories by the National Voluntary Laboratory Accreditation Program. Modules are tested against FIPS 140-2 security requirements covering 11 areas, including implementation of FIPS-approved algorithms, specific management of the decryption key lifecycle, approved generation of random numbers, and self-testing.

Within most areas, a cryptographic module receives a security level rating (1-4, from lowest to highest), depending on the requirements met. For areas that do not provide for different levels of security, a cryptographic module receives a rating that reflects fulfillment of all of the requirements for that area. FIPS 140-2 validations apply only to a specific version of software running on a specific version of hardware.

The great value of this program is demonstrated by the fact that, according to the 2011 *NIST Computer Security Division Annual Report*, 61 percent of cryptographic modules tested in that year had security flaws that were able to be corrected during testing. In the DoD, IT administrators now require FIPS 140-2 validation for all products.

Cisco's Commitment to Certification

Cisco is the recognized leader in security certifications, with more product certifications than any other IT vendor in the world. These programs include cryptographic algorithm implementation validation through the FIPS 140-2 standard, Common Criteria, and the Approved Products Lists (APLs) for global governments, including U.S. Defense Information Systems Agency (DISA) and NATO's Information Assurance Product Catalog (NIAPC).

Cisco invests millions of dollars annually in the product certification process to meet these rigorous standards. Its encryption capabilities are a basic feature in more than 80 families of Cisco products, offering an end-to-end, fully compliant network architecture. These include FIPS certification for the switching, routing, and collaboration

product families that are referenced within Cisco's best practices documentation for building a Medical-Grade Network.

The Cisco® Medical-Grade Network is a set of Cisco recommended guiding principles that can be used to build a network foundation that enables reliable, seamless, and secure communications within the healthcare community. This framework allows integration and interoperability at each functional area to optimize and safeguard interactions among participants, processes, applications, and hardware components. It also supports secured connectivity with business associate organizations, such as acute care campus networks, ambulatory clinics, remote clinicians, and data centers, as required by the HIPAA standard.

It is also important for network vendors to play a role in helping to define the ongoing certification process and to advise government and business as new capabilities emerge. Cisco is a leading member of the Trusted Computing Group, the Open Group, the Institute of Electrical Engineers (IEEE), and the Internet Engineering Task Force (IETF), and works closely with governments worldwide. These organizations provide the international leadership required to create ongoing standards for information security and encryption.

Conclusion

Any vendor can assert that its system is secure by claiming that it uses the highest encryption technologies available. Given the public visibility of breaches of trust, there is no reason to risk exposure with systems that do not meet the FIPS 140-2 standard for information encryption. Without this validation, the network's cryptography function has a demonstrated a less than 50 percent chance of being implemented correctly. The FIPS validation process gives healthcare providers a new level of confidence in the security of their critical data, allowing them to reduce risk without increasing costs.

As a leader in the healthcare networking industry, Cisco will continue to play a major role in encryption development, keeping healthcare systems secured both now and in the future. Visit our website to learn more about Cisco Global Government Certifications.

For more information on Cisco and healthcare, visit our Healthcare Industry Solutions page or contact your local account team.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-718995-00 11/12