



## Secure Messaging for the Healthcare Industry Coming to Grips with HIPAA

Voltage Security, Inc.  
September 2004

**Copyright © 2004 Voltage Security, Inc.**

All rights reserved.

All information in this document is subject to change without notice. This document is provided for informational purposes only and Voltage Security, Inc. makes no warranties, either express or implied, in this document.

SecureMail, SecureFile, SecureIM and SecurePolicy Suite are trademarks of Voltage Security, Inc. All other company and product names may be trademarks of their respective owners.

## Table of Contents

HEALTHCARE PRIVACY AND SECURITY A NATIONAL CONCERN .....	3
THE FUTURE: ELECTRONIC MEDICAL RECORDS INSTANTLY AVAILABLE .....	3
HIPAA AND HEALTHCARE SECURITY BACKDROP.....	4
DELIVERING HEALTHCARE THE IT WAY .....	5
TECHNICAL SECURITY CONTROLS .....	6
VOLTAGE SOLUTIONS FOR HIPAA REQUIEMENTS .....	6
CONCLUSION.....	7
APPENDIX .....	8

## Healthcare Privacy and Security a National Concern

Few records are more sensitive to the public than medical records. Patients demand the peace of mind that comes with knowing that organizations that collect medical information adhere to a promise to keep the data confidential. Unfortunately, the history of medical records management demonstrates that privacy and security breaches occur regularly. Consider some examples:

- A health care worker stole the paper medical records of the famous tennis star, Arthur Ashe, photocopied them, and sold them to a newspaper. The newspaper then publicized Ashe's HIV status. He felt compelled at that point to announce his condition to the public.<sup>1</sup>
- Paper records are not the only ones at risk. Eli Lilly, a pharmaceutical company based in Indiana, inadvertently disclosed sensitive personal information collected from consumers through its Prozac.com Web site. The company disclosed e-mail addresses of 669 subscribers to its Prozac Reminder Service.<sup>2</sup>
- A public health worker in Tampa, Florida stole a list of 4,000 HIV-positive people on a computer disk and sent the names to two newspapers.<sup>3</sup>

Incidents such as these led Congress to add privacy and security protections for health information into the Health Insurance Portability and Accountability Act (HIPAA).<sup>4</sup> HIPAA calls for finalizing comprehensive privacy and security standards, which the Department of Health and Human Services (HHS) has established. Although the HHS privacy regulations became effective on April 14, 2003 and the security regulations have a compliance deadline of April 21, 2005, many entities covered by HIPAA have not completed compliance programs and are just now coming to grips with the privacy and security standards.

## The Future: Electronic Medical Records Instantly Available

Dramatic change is in store for health care. The US Government has announced sweeping changes to move the nation towards the ubiquitous use of electronic medical records. The President created a National Health Information Infrastructure (NHII) to promote the use of electronic medical records as part of an effort to improve the quality and efficiency of health care.<sup>5</sup> The idea is to make up-to-date health records instantly available, whenever and wherever they are needed.<sup>6</sup>

The NHII initiative promises to allow different parts of the health care system to rapidly communicate for enhanced care. For example, caregivers for someone on vacation needing emergency care can alert and consult with the patient's primary care physician back home electronically, view the patient's medical records online, and add patient notes and instructions that the patient can view later online. The caregivers can also correlate the patient's condition with other public health information sources to analyze possible patterns and identify possible health risks to the public. If public health risks are identified the provider can swiftly, through email or other electronic methods, disperse the information to the necessary parties. Another example is the routine electronic communication among patient,

---

<sup>1</sup> Janlori Goldman, Dir., Health Privacy Project, Instit. for Health Care Research and Policy, Georgetown Univ., Testimony Before the House Subcomm. on Health, Comm. on Ways and Means, March 24, 1998.

<sup>2</sup> Federal Trade Commission press release < <http://www.ftc.gov/opa/2002/01/elililly.htm>>.

<sup>3</sup> Univ. of Texas Southwestern Medical Center, "What Price Privacy? . . . Invaluable!" SOUTHWESTERN COMPLIANCE NOTES, vol.2, no. 4.

<sup>4</sup> Health Insurance Portability and Accountability Act of 1996, Pub. Law No. 104-191, Statutes at Large ("Stat."), vol. 110, p. 1936 (1996).

<sup>5</sup> Executive Order 13335 (Apr. 27, 2004), reprinted in Federal Register, vol. 69, no. 84, p. 24,059 (Apr. 30, 2004).

<sup>6</sup> HHS Press Office, "Harnessing Information Technology to Improve Health Care" p. 1 (HHS fact sheet May 6, 2004) ["HHS Fact Sheet"].

doctor, and pharmacy. A doctor can electronically (via email) prescribe medication and, in real time, receive alerts about the latest information on adverse drug reactions to catch problems before they occur.<sup>7</sup>

As promising as NHII sounds, a critical component of that effort is ensuring the security and privacy of individually identifiable health information. Accordingly, the NHII will involve its own security and privacy standards.<sup>8</sup> These standards will augment existing HIPAA privacy and security requirements. The bottom line is that with HIPAA security regulations and emerging standards, integrating security solutions with advances in information technology is a must.

## HIPAA and Healthcare Security Backdrop

HIPAA is the principal law today governing the privacy and security of electronic health care-related information. As one of the many things it includes, HIPAA contains “administrative simplification” provisions to foster the use of electronic transactions for the communication of health information to improve the efficiency and effectiveness of the health care system.<sup>9</sup> In 2000, HHS issued final regulations on privacy (Privacy Rule), and in 2003, HHS issued final regulations on security (Security Rule) for electronic health information.<sup>10</sup> HIPAA covers health plans, healthcare Clearinghouses, and health care providers who transmit information in electronic form for certain kinds of transactions (Covered Entities).<sup>11</sup>

HIPAA calls for standards requiring Covered Entities to implement “appropriate administrative, technical, and physical safeguards.” The purpose of these safeguards is to ensure the integrity and confidentiality of health information. The safeguards also are to protect against reasonably anticipated threats and unauthorized uses.<sup>12</sup> The Privacy Rule, which became effective in 2003, has already used similar general language to impose security requirements on Covered Entities. The Privacy Rule mandates the protection of “Protected Health Information” (PHI). The Privacy Rule says PHI includes electronically transmitted or maintained records, as well as information transmitted or maintained in any other medium,<sup>13</sup> which presumably includes paper.

The Security Rule imposes the same general requirements of confidentiality, integrity, and availability on Covered Entities with respect to electronic PHI (electronic PHI). The Security Rule goes on to fill in some detail with a set of high level “standards” the Covered Entities must meet.<sup>14</sup> These standards address administrative, physical, and technical security controls, as well as organizational requirements and documenting policies and procedures. More detailed “implementation specifications” in turn flesh out the standards. Some of the implementation specifications are “required” while others are merely “addressable.” A Covered Entity needs to implement “addressable” specifications if they are “reasonable and appropriate.” If they are not, a Covered Entity can comply instead simply by documenting the reasons why they are not reasonable and appropriate, and implement any alternatives

---

<sup>7</sup> The National Committee on Vital and Health Statistics Workgroup on the National Health Information Infrastructure, *Toward a National Health Information Infrastructure* (Jun. 2000) <<http://www.ncvhs.dhhs.gov/NHII2kReport.htm>>.

<sup>8</sup> HHS Fact Sheet at p. 1; see Executive Order 13335, secs. 2(f), 3(a)(iv).

<sup>9</sup> HIPAA § 261, 110 Stat. at 2021.

<sup>10</sup> Code of Federal Regulations (“C.F.R.”), title 45, parts 160, 164).

<sup>11</sup> United States Code (“U.S.C.”), title 42, sec. 1320d-1(a); 45 C.F.R. § 160.102(a).

<sup>12</sup> 42 U.S.C. § 1320d-2(d)(2).

<sup>13</sup> 45 C.F.R. § 160.103 (definition of “Protected Health Information”). PHI refers to health information created or received by a Covered Entity relating to the medical condition, health, or care of an individual, where the individual can be identified in the information, and where the information is electronically transmitted or maintained, or transmitted or maintained in any other medium.

<sup>14</sup> 45 C.F.R. § 164.306(c).

security controls that are reasonable and appropriate.<sup>15</sup>

As mentioned above, however, the new National Health information Infrastructure will add privacy and security standards to HIPAA. Consequently, HIPAA will only be one part of the overall health care security regulatory picture. In addition, the recent Medicare modernization legislation funded a pilot to explore the use of email and other alerts and reminders for delivering health care to Medicare patients.<sup>16</sup> The Medicare legislation also called for HHS to develop standards for electronic prescriptions, consistent with the Privacy Rule, and authorized HHS to fund grants to assist physicians to implement electronic prescription programs.<sup>17</sup> These new health information technology programs may also involve their own security requirements, standards, or guidelines.

## Delivering Healthcare the IT Way

Information technology and the Internet moved the sale of consumer products from bricks-and-mortar stores and mail order to the online world. IT and the Internet can and will do the same for the delivery of health care. Patients won't use online systems, however, unless providers assure the security and privacy of their patients' records. With security assurances, though, providers can deliver more care, faster, and more efficiently. By driving down the cost of delivering medical care, they can reach more patients who can't afford traditional office visit-oriented health care. By going online, providers can expand the geographic reach of their patient base to rural and underserved areas. Premier institutions, like the Mayo Clinic, can use IT to support a national patient base.

Consider a few examples of delivering health care using information technology:

- **Online Consultations:** New pilots and private initiative are underway to allow doctors to consult with patients online and obtain reimbursement from Payors. Blue Cross Blue Shield of Florida will pilot a program with 3,000 doctors to reimburse them for online medical consultations. Patients can log onto a secure web site and tell their doctors about non-urgent problems and receive advice. The programs can cut the frequency of office visits, and a Stanford study showed that online consultations cut total health care claims by an amount more than \$3 per member per month.<sup>18</sup>
- **Provider to Provider Communication:** Providers need to communicate with other providers quickly and efficiently. Providers commonly write consultation letters or refer a patient to a specialist by postal mail. Moving a patient's records from one office to another can currently involve postal mail, fax, or even physically carrying the records. While providers may have electronic access to lab results within their own health systems, lab results (including blood and cholesterol tests) are harder to move from one system to another. In the future, providers can use secure email and other technologies to consult and refer patients. Labs can push results to doctors via secure email or allow doctors to pull them down. And the NHII will allow providers in one system to access medical records in another system.
- **Electronic Prescriptions and Renewals:** The age-old method of a doctor giving the patient a handwritten prescription for the patient to walk the prescription into a pharmacy for filling is both an inefficient way to transport the prescription; it also leads to the danger of the pharmacist misinterpreting the doctor's handwriting. In the future, doctors will be able to record prescriptions electronically to eliminate handwriting mistakes, and send them to pharmacies securely via secure messaging. Patients will receive their prescriptions faster with fewer errors.

---

<sup>15</sup> 45 C.F.R. § 164.306(d).

<sup>16</sup> Medicare Prescription Drug, Improvement, and Modernization Act of 2003 § 649(a)(1), (h)(2) ["MMA"].

<sup>17</sup> MMA § 101 (codified at 42 U.S.C. § 1395w-104(e), (e)(2)(C)).

<sup>18</sup> Laura Landro, *The Doctor is Online: Secure Messaging Boosts the Use of Web Consultations*, WALL STREET JOURNAL, Sept. 2, 2004, at D1.

## Technical Security Controls

While new developments in the use of health information technologies for electronic records, care delivery, and prescriptions raise the possibility of additional regulatory guidance, the HIPAA Security Rule has a more immediate effect. Companies seeking to upgrade their technical security controls for health care security today can turn to the Security Rule to understand their responsibilities as of April 21, 2005. With respect to the security of electronic PHI in transit or at rest, the Security Rule contains a list of technical security controls and related administrative security controls.

Technologies already exist to help Covered Entities meet these security controls. These technologies can permit a Covered Entity to:

- Control access to electronic PHI to prevent unauthorized disclosure to intruders or personnel not authorized to see it.
- Facilitate the encryption of electronic PHI in transit or at rest.
- Use authentication mechanisms to confirm the identity of users, facilitate the security of authentication tokens such as passwords, and ensure accountability of users by assigning them unique identifiers.
- Implement integrity controls over electronic PHI to ensure that if any attacker or accidental process alters or destroys electronic PHI, the alteration or destruction would be detected.
- Manage security through tools for provisioning user access and for changing or removing access as needed.
- Maintain an audit trail of activity to detect and provide an evidentiary record of user activity.

## Voltage Solutions for HIPAA Requirements

Voltage Security, provides a privacy platform that allows the healthcare industry to meet messaging security and privacy concerns head on. The Voltage Privacy platform enables you to secure multiple methods of communication under a single policy framework that is flexible enough to accommodate the full range of participants – labs, doctors, nurses, patients, and vendors. providers, payors and business associates can encrypt and send secure electronic patient and physician information, without certificates, passwords, or the complexity of PKI.

The Voltage Privacy platform is based on award-winning technology – Identity-Based Encryption (IBE) that eliminates the need for certificates, requires no change in end user behavior, can integrate with most any network infrastructure, and enables security across a variety of channels controlled under a single policy framework.

Voltage SecureMail and SecureFile enable healthcare organizations to exchange sensitive information seamlessly, swiftly, and securely either with an integrated plug-in or without any software download. Voltage SecureMail Gateway enables Covered Entities to identify the policies that govern which emails will automatically be sent out securely. In addition Voltage SecureMail for the Blackberry enables organizations to send out secure email through their mobile devices such as BlackBerry.

All Voltage security solutions contain the critical security technologies to enable customers to implement the safeguards in the HIPAA Security Rule. The table in the Appendix maps the security controls in HIPAA with security technologies that can address these controls, and shows how Voltage solutions provide these technologies to protect patient information. No set of technologies provide HIPAA security compliance “in a box.” Yet using Voltage technology can play a critical role in an overall HIPAA compliance program by securing different kinds of point-to-point communications and file management.

## Conclusion

The nation is overhauling the way it delivers health care. The government is fostering programs to integrate information technology into the way health care is delivered. Security and privacy must go hand-in-hand with advances in health care information technology. Not only does the HIPAA security rule impose technical security requirements, the new National Health Information Infrastructure will impose its own security standards. Voltage is a solutions provider whose secure mail, secure file transfer, and secure instant messaging technologies will enable Providers, Clearinghouses, and Payors to transmit and store health records securely, while enabling them to take advantage of the efficiencies, cost-savings, and larger markets that come with the integration of IT into health care.

### About Voltage Security

*Voltage Security is a new information security company focused on developing innovative solutions to address the challenges of securing business critical communication. Voltage is the first to use identity to bring confidence to business communication. Voltage solutions make anytime, anywhere business communication easy to use and painless to deploy. Voltage Security is based in Palo Alto, California.*

*For more information, please visit [www.voltage.com](http://www.voltage.com), email [info@voltage.com](mailto:info@voltage.com) or call +1 650 543 1280*

## Appendix

This table maps the technical and some of the related HIPAA security controls with the Voltage solution.

### Technical Security Controls and Voltage's Solution for Electronic PHI

Type of Safeguard	Voltage Solution
<b>Confidentiality and Access Control</b>	
Covered Entities must implement access control measures to limit electronic PHI access to authorized persons or applications. <sup>19</sup> <b>Standard (required).</b>	The Voltage Privacy platform uses IBE technology to easily encrypt and limit access to electronic PHI to users possessing the validated proper credentials and associated access rights, wherever the PHI data may reside. Unlike traditional security solutions such as PKI, web-based or symmetric solutions, this is done without having to manage certificates, individual message keys or web mail storage. Voltage Security solutions are flexible in supporting the determined policies and procedures for granting access to electronic PHI.
Where reasonable and appropriate, Covered Entities must implement policies and procedures for granting access to electronic PHI, such as through workstations and applications. <sup>20</sup> Addressable implementation specification.	
If reasonable and appropriate, Covered Entities must implement controls on creating, changing, and safeguarding passwords. <sup>21</sup> Addressable implementation specification.	Voltage Privacy platform provides a management console for setting and administering policies, tracking private key requests, and integrating with authentication or identity management solutions. No other solution offers the flexibility and control of authentication for people inside and outside the firewall.
If reasonable and appropriate, Covered Entities must implement encryption of electronic PHI. <sup>22</sup> Addressable implementation specification.	The Voltage Privacy platform enables permits Covered Entities to easily encrypt and decrypt email, files and instant messages without the burden of managing complex security information (e.g., certificates) for individuals. Voltage solutions permit the transmission of various communications to individuals or groups in an encrypted state, which only the authorized recipient(s) can decrypt. Furthermore, all content secured with Voltage solutions are stored encrypted wherever they may rest (e.g. mail server, portals, etc.)
A Covered Entity must prevent unauthorized access to electronic PHI being transmitted over a network. <sup>23</sup> <b>Standard (required).</b>	

<sup>19</sup> 45 C.F.R. § 164.312(a)(1); see 45 C.F.R. § 164.308(a)(4)(i).

<sup>20</sup> 45 C.F.R. § 164.308(a)(4)(ii)(B).

<sup>21</sup> 45 C.F.R. § 164.308(a)(5)(ii)(D).

<sup>22</sup> 45 C.F.R. § 164.312(a)(2)(iv), (e)(2)(ii).

<sup>23</sup> 45 C.F.R. § 164.312(e)(1).

Type of Safeguard	Voltage Solution
<b>Integrity</b>	
Covered Entities must implement policies and procedures to protect the integrity of electronic PHI and prevent improper alteration or destruction. <sup>24</sup> <b>Standard (required).</b>	All Voltage secured communications and files are digitally signed with standard DSA signatures. This ensures the integrity of the communication and authenticates the sender. Voltage solutions will verify authenticity and data integrity and alert the recipient should tampering of the message have occurred.
The integrity controls must, if reasonable and appropriate, include electronic mechanisms to confirm that electronic PHI has not been altered or destroyed. <sup>25</sup> Addressable implementation specification.	
The integrity controls must, if reasonable and appropriate, include integrity controls for electronically transmitted electronic PHI. <sup>26</sup> Addressable implementation specification.	
<b>Authentication</b>	
Covered Entities must assign each user a unique user identification (name or number) to track user identity. <sup>27</sup> Required implementation specification.	Voltage solutions permit Covered Entities to issue a unique key pair to each user based in part on a simple identifier such as an email address. Voltage solutions leverage existing identity management solutions and provide the flexibility to choose the form of centrally managed authentication for such users. Examples of such authentication schemes include Active Directory, LDAP, two-factor authentication, email answerback authentication, Question and Answer authentication and any custom authentication scheme that the covered entity may have implemented.
Covered Entities must use procedures to verify that a person or entity accessing electronic PHI is who he, she, or it purports to be. <sup>28</sup> <b>Standard (required).</b>	The Voltage solution centrally determines the authentication mechanism required to obtain private keys, and thereby ensures that only authorized entities can access data protected by Voltage technology.
<b>Security Management</b>	
Information systems must implement audit controls through hardware, software, or procedural mechanisms in order to record or examine activity. <sup>29</sup> Standard (required).	The Voltage SecurePolicy Suite logs administrator activity and key issuance events. Examples of key issuance events that are tracked include who has requested the private key, when it was requested, where it was requested from and the end result of the key request.

<sup>24</sup> 45 C.F.R. § 164.312(c)(1).

<sup>25</sup> 45 C.F.R. § 164.312(c)(2).

<sup>26</sup> 45 C.F.R. § 164.312(e)(i).

<sup>27</sup> 45 C.F.R. § 164.312(a)(2)(i).

<sup>28</sup> 45 C.F.R. § 164.312(d).

<sup>29</sup> 45 C.F.R. § 164.312(b).

<p>If reasonable and appropriate, the Covered Entity must implement access control policies and procedures to document, review, and modify privileges for access to assets such as workstations and applications.<sup>30</sup> Addressable implementation specification.</p>	<p>The Voltage SecurePolicy Suite provides a management console for setting and administering policy, tracking private key requests, and configuring the means of end user authentication. The administrator can set security settings for client application, implement variable authentication policies for different groups, and set the frequency of mandatory re-keying and/or re-authentication.</p>
--	--

#### About Voltage Security

*Voltage Security is a new information security company focused on developing innovative solutions to address the challenges of securing business critical communication. Voltage is the first to use identity to bring confidence to business communication. Voltage solutions make anytime, anywhere business communication easy to use and painless to deploy. Voltage Security is based in Palo Alto, California.*

*For more information, please visit [www.voltage.com](http://www.voltage.com), email [info@voltage.com](mailto:info@voltage.com) or call +1 650 543 1280*

---

<sup>30</sup> 45 C.F.R. § 164.308(a)(4)(ii)(C).