

**White Paper**

**Healthcare, E-mail**  
**and HIPAA Security Requirements**



© 2001-2002 CertifiedMail.com, Inc.

<http://www.re-soft.com>

## **E-Mail In Healthcare**

According to industry estimates, more than half of the US population is currently using Internet e-mail, and more than 40 percent of patients use e-mail to contact health professionals.<sup>1</sup> Increasingly, e-mail is taking the place of phone calls to communicate between doctors and patients. The latest results of the Internet Survey of Medicine<sup>2</sup> revealed that 85 percent of physicians surveyed are currently using the Internet, more than 63 percent of the physicians surveyed use e-mail daily, and 33 percent have used e-mail to communicate with patients. E-mail is also popular with healthcare workers to send patient data and attachments to colleagues and medical facilities for collaboration and review. E-mail empowers the healthcare industry in new ways and brings new expectations as well.

Significant productivity gains and cost savings will further entrench e-mail into the healthcare industry. But before e-mail can be used as a universal communication tool for sensitive data, several significant drawbacks must be addressed. E-mail was designed for easy, rapid flow of information, without considering accountability and security of information. These are important attributes to the healthcare industry, especially when sending patient-related information. In the same way that patient medical records would never be sent on the back of a postcard, e-mailing the same data exposes this information as plain text to the Internet.

Fortunately, the limitations of e-mail are already known to many in the healthcare industry. The American Health Information Management Association, in their E-mail Draft Policy, indicates that “E-mail communication systems are not secure; mail sent via the Internet or other external systems can be intercepted and read by individuals other than the intended recipient.” Federal legislators are also aware of these limitations, and have passed new regulations ensuring the privacy of patient data.

## **HIPAA Overview**

The Health Insurance Portability & Accountability Act (HIPAA) is a new federal regulation that mandates the privacy of health data. HIPAA is resulting in sweeping changes in most healthcare transaction and administrative information systems. Affected organizations includes all health care providers, even one physician offices, health plans, employers, public health authorities, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations, and universities. E-mail is one of the primary systems affected by this legislation.

---

<sup>1</sup> E-mail Contact Between Doctor and Patient. Medical Practice Communicator (1999)

<sup>2</sup> Healthcon Corp.



It has been estimated that HIPAA compliance will consume 33 cents of every healthcare dollar spent between now and 2003.<sup>3</sup> HIPAA must be taken seriously, as it includes civil and criminal penalties for non-compliance, including fines up to \$25K for multiple violations of the same standard in a calendar year, and fines up to \$250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information.

### **CertifiedMail Solution**

The ideal scenario for healthcare organizations would be to maintain the benefits of their existing e-mail system, expand its use to gain more efficiency, and comply with HIPAA requirements. By leveraging widely adopted open standards for security, and supplementing existing e-mail systems with these standards, this ideal scenario can be attained.

CertifiedMail.com Inc. is a security company that provides HIPAA-compliant e-mail for healthcare organizations. Based on open standards, CertifiedMail enables enterprises to rapidly establish secure, accountable, scalable communication with thousands or millions of recipients, including customers, colleagues and vendors. The CertifiedMail solution is installed in the organization's DataCenter, and enhances existing e-mail platforms. With CertifiedMail, healthcare employees use their current e-mail client, such as MS-Outlook or Lotus Notes, to send secure e-mail. This eliminates the need for retraining, and results in rapid adoption. Another key feature is ease of use for Internet-based recipients and patients, and employees who are traveling or at home, with no special system requirements or software to download.

The CertifiedMail solution is designed to be easy and ubiquitous, yet offer the high level of security needed to comply with privacy regulations. Features such as end to end message security, transparent encryption, digital fingerprints to verify document originality, strong authentication of senders and recipients, and two-factor authentication with smart cards, X.509 certificates and SecurID provide a very robust security environment. But even with these advanced features, a security system should be easy to use by senders, recipients and By leveraging open standards, using decades of experience in software and security design, and continually learning from customer feedback, the CertifiedMail system is easy for administrators to manage and maintain, and for users to send, receive and track secure e-mail.


---

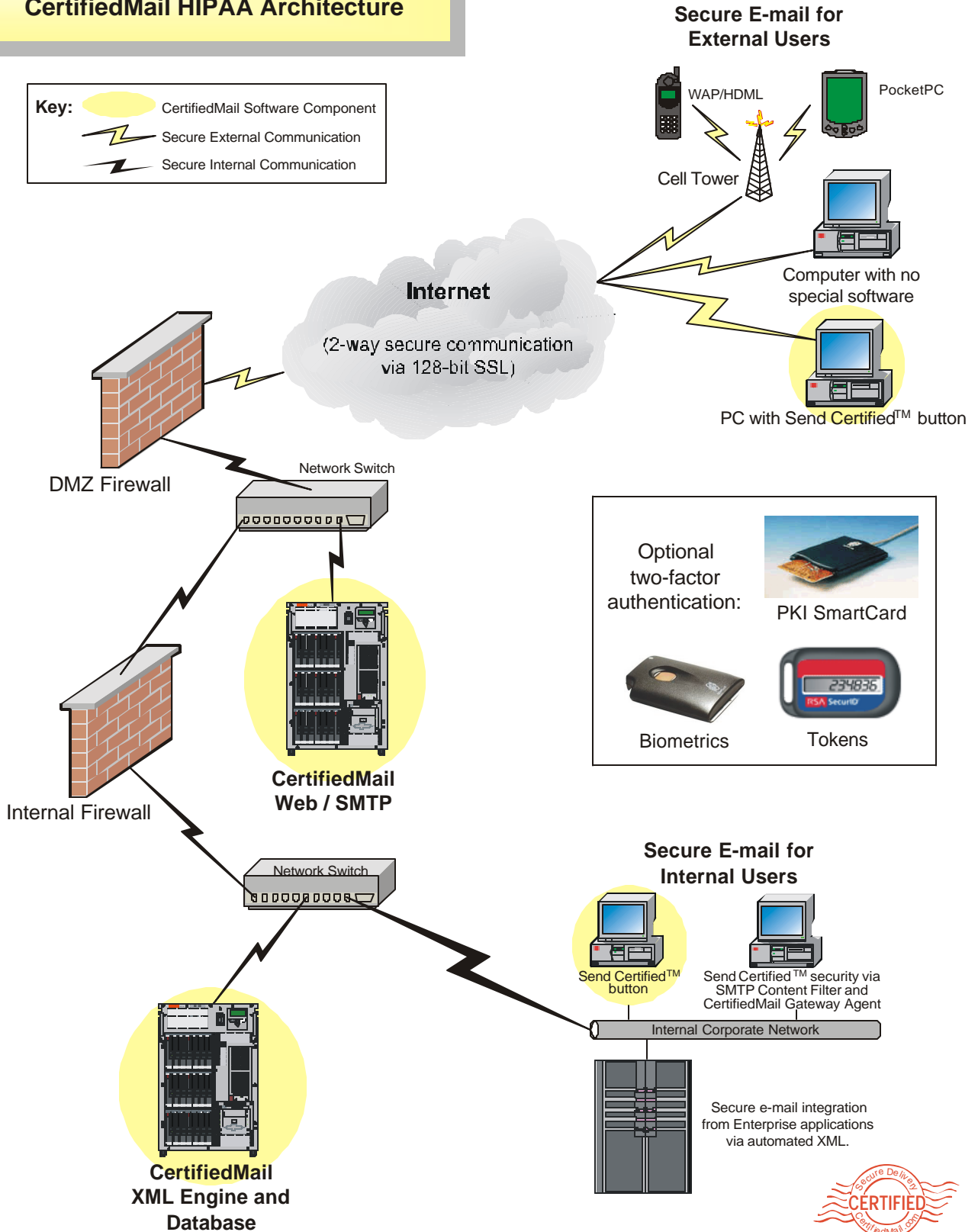
<sup>3</sup> HIPAAsource content provided by [Phoenix Health Systems](#) and [HIPAAdvisory.com](#)

### Appendix A

## CertifiedMail HIPAA Architecture

**Key:**

-  CertifiedMail Software Component
-  Secure External Communication
-  Secure Internal Communication



## Appendix B

Following are key elements of the CertifiedMail HIPAA-compliant messaging system.

Design Element	CertifiedMail	Benefit
<b>Secure Messaging Implementation</b>		
E-mail client integration	Send Certified button for Outlook, Lotus Notes and Exchange	One-click security from popular e-mail clients eliminates training and mistakes.
E-mail Gateway interface	Yes	Supports policy-based content filters. No client software needed to send secure messages from the desktop.
Wireless Support	Yes	All secure messaging features have been extended to WAP/HDML-enabled devices such as Internet cell phones.
Authentication, Encryption, Integrity	Yes	User Authentication, end-to-end transparent encryption and message integrity using RSA MD5 digital fingerprint.
RSA SecureID Authentication	Yes	Integrate the CertifiedMail login with your existing SecureID ACE Server, providing strong user authentication.
PKI Authentication	Yes	PKI certificates can be queried for strong authentication.
eSign Electronic Signatures	Yes	Embed digital signatures into documents and HTML pages in compliance with the eSign Act.
Any Internet recipient can receive a secure message	Yes	Universal system-wide secure e-mail platform.
Message tracking	Yes	Confirmation when the recipient opened your message.
Retract message not yet opened.	Yes	Undo costly errors when e-mail is sent to the wrong recipient.
Unlimited attachments per message	Yes	Transmit any number of attachments, including very large documents, even though the recipient's e-mail system has message size or storage space limitations.
<b>Server Technology</b>		
OS platform	Intel-based servers and Windows 2000 operating system	Low cost hardware, software and on-going maintenance. Enterprise ready. (e.g. NASDAQ 2+ billion transactions/day on Windows 2000 systems.) Easy to maintain.
Data interfaces	XML, SQL and SMTP	Rapid integration with legacy systems and enterprise applications, including call center and billing systems.
Enterprise Version	Yes	Fault-tolerant, clustered and load-balanced configuration installed in your DataCenter.
Department Version	Yes	Appropriate for departmental usage, and can be upgraded to a full server without losing data.

