



---

# Privacy, Security and HIPAA

A Common Sense Approach to  
Meeting HIPAA Standards

Authora Inc.  
1959 NW Dock Place  
Seattle, WA 98107  
Phone: 206.783.8000  
[www.authora.com](http://www.authora.com)

## **Background - Internet Privacy, Security and HIPAA**

The idea of passing individual health records across the public Internet has prompted legitimate concerns about the privacy and security of patient-identifiable information-- also called "protected health information" (PHI). As a result, The Health Insurance Portability and Accountability Act ("HIPAA" or the "Act") has called for privacy and security standards in regards to sharing PHI in electronic form.

### **Who needs to be HIPAA compliant :**

HIPAA impacts any healthcare entity, large or small, that exchanges individually identifiable health information. This includes entities such as providers, payers, and clearinghouses or other entities such as laboratories, billing agencies, IT vendors, employers, pharmaceutical and biotechnology companies.

### **Compliance deadline of April 14, 2003 :**

Covered entities are currently facing a deadline of April 14, 2003 for compliance with the privacy rule. (Small health plans have been given an additional year to comply.) While a deadline for compliance with the security standard is not yet established, the standard is in a proposed form and is expected to be finalized this August.

### **Scoping the impact on an organization:**

To understand how the HIPAA privacy and security requirements impacts an organization, one needs first to understand how protected health information comes to an organization, how it's used, and how it flows to the outside world. At the end of the day, an organization must be in a position to answer questions posed by a patient or other parties responsible for protecting a patient's information including:

- Who has PHI at any point during its lifecycle?
- What will they use it for?
- What procedures does an organization have in place to track the flow of information?
- If an organization doesn't have mechanisms in place to track information, what assurances does it have from business associates and others that information is going to be used appropriately?
- How does an organization verify the identity/authority of users and requesters?

### **Authora: a Common Sense Approach to HIPAA**

Authora's products and services were built with the understanding that Privacy and security are inextricably linked. Although the security deadline for HIPAA compliance is not yet

decided, it is important to consider compliance measures for **both** privacy and security. Covered entities that take the appropriate steps to address both of these regulations (privacy & security) will benefit not only from compliance with HIPAA but will experience a return on investment by moving business processes online.

To ensure the privacy of patient information security controls need to be in place. For example, if an organization must transmit data to a business associate, two things must happen: (a) the organizations must enter into an agreement regarding the use of the data (privacy), and (b) when the data is transmitted, the organizations must ensure that the data gets to the business associate safely (security).

Authora's common sense approach to HIPAA privacy and security compliance can reduce an organization's costs, improve the quality of patient care, reduce an organization's liability exposure and increase consumer satisfaction.

### **The Challenges:**

#### **Ensuring the Privacy and Security of Patient Health Information Outside Your Organization**

HIPAA privacy and security standards apply to all personally identifiable health information distributed in an electronic format, whether it be in the form of e-mail messages, Web content, or documents. The open nature of the Internet makes it extremely difficult to control and manage e-mail and attachments that are exchanged daily with outside business associates and other entities. As a result, the risk of intentional or accidental disclosure of patient information through e-mail communication is extremely high. Written corporate e-mail policies can curb the disclosure of PHI, but they aren't a substitute for deploying an information security solution.

From an information technology perspective, an organization's messaging environment represents a huge security challenge. The complex nature of a messaging environment makes it difficult to apply security since it requires:

- Preserving the sender's existing e-mail work flow
- Providing recipients with a seamless way to view protected e-mail and attached documents
- Protecting messages automatically and transparently so that the enforcement of corporate e-mail policies is not at the discretion of individual e-mail users
- Introducing new security mechanisms with minimal to no impact on IT administration

#### **Authora's Simple Solutions for HIPAA compliance**

Authora's secure messaging solutions address all of the above healthcare security requirements while providing flexible deployment options to adapt to disparate recipient e-mail environments. Authora's secure messaging solutions combine policy management capabilities with strong encryption, Authentication and access controls. This unique combination of features gives healthcare entities unprecedented flexibility and control over how sensitive patient information is accessed, used and managed across the Internet.

**Authora's secure messaging solutions meet the following key requirements for exchanging PHI over the Internet:**

- Applies encryption, Authentication, and authorization controls to e-mail, attachments, webforms, or webpages to ensure their integrity
- Secures e-mail or other data without impacting an organization's existing workflow. Policies and Middleware works with existing content scanning engines, mail servers, or webservers and applies HIPAA compliance protection based on specific terms such as patient social security numbers. *(See Preserving a Healthcare Entity's Existing Workflow below)*
- Enables data to be protected and delivered by securing middleware Web servers, Mail Servers or Mail Clients. Recipients can view and reply to protected e-mail or webforms using a standard Web browser
- Extends protection to e-mail after it's delivered to a recipient's Inbox. This protection includes the ability to track and audit message activity; and, expire e-mail or data.
- Provides auditing capabilities to ensure that patient information has been properly disclosed in accordance with existing corporate policies
- Provides "plug-and-play" integration with an organization's existing Authentication infrastructure

**Preserving a Healthcare Entity's Existing Workflow**

One of the most critical messaging requirements for any healthcare organization is the ability to secure content transparently without impacting an entity's existing workflow.

Organizations don't want to affect the manner in which users send or receive data.. Authora addresses this issue by integrating with backend systems and end users computers seamlessly. An e-mail scanning engine typically resides between an organization's mail server and the Internet and scans messages for inappropriate language, viruses and other functions. Authora's secure messaging solution works in concert with content scanning engines and outbound e-mail containing PHI can be directed to the Authora Sovereign Server. Messages that contain PHI are encrypted and protected on Authora's EDGE (encrypted Data Gateway Engine) Server and delivered to the recipient.



for e-mail messages and attachments, or webforms in html and xml allowing messages to be continuously protected and controlled after they are delivered to recipients. For example, a sender can expire e-mail messages or change a recipient's access privileges (e.g. print, copy/paste) anytime after delivery.

## How It Works

Authora's secure messaging system offers three deployment options. This system gives enterprises the flexibility to automatically secure PHI without any user involvement or to provide individual users with the ability to protect and manage their own messages and documents. The solution can be deployed through:

- **Zendit's Trustpoint Enterprise Suite™** A simple solution for protecting intra, inter and extra net data, including authentication, intelligent access right enforcement, encryption and digital signatures, consists of Trustpoints and the Encrypted Data Gateway engine (EDGE). Trustpoints plug in to existing enterprise servers and send sensitive outbound data through the "encrypt, digitally sign, and deliver" process, (or if it's inbound data, through the "decrypt, verify signature, and deliver to existing business process) Trust Points can be installed on application servers or on stand-alone servers. Sensitive financial and medical HTML & XML data is efficiently risk managed. Trust points complement and work in conjunction with Zendit's enterprise Sovereign Server, Encrypted Data Gateway, and end user Trust Agents. The following is a description of a few Zendit Trust Points:

- **SMTP** – Seamlessly encrypts and/or digitally signs outbound SMTP email. No client is installed in the user's email programs. All selected email, including batch email notifications, can be automatically encrypted so only the recipient can read it, ie. transaction notifications or balance statements. Uses single corporate lock and key.
- **POP3** – Seamlessly decrypts and/or verifies digitally signed incoming email. No client is installed in the user's email programs. Uses single corporate lock and key.
- **Exchange** – A Microsoft Exchange 2000 server security enhancement. Seamlessly encrypts and/or digitally signs outbound email and decrypts and/or verifies digitally signed incoming email. Can use either a single corporate lock and key or individual locks and keys.
- **File** – Files on local server shares or FTP directories are automatically encrypted for safekeeping. Users can decrypt the files with the proper authority set by the policies in the Trust Zone.
- **HTML** – Works with a web server and encrypts and/or digitally signs sensitive web page content for decryption by the client. Example: a user logs into a bank account summary page, an encrypted block is displayed on the page, the DZendit button is selected and the page is decrypted verified and displayed.
- **XML** – XML data is seamlessly encrypted and/or digitally signed for secure delivery and decryption on the client. [not sure what the meaning was here for XML, so I might not have fixed anything]
- **Web Entry** – Next generation of authentication. A digital signature web access control scheme wherein the user "drags and drops" a digital key/digital identity off the surfboard onto a web page. The web page generates a random number, which is

signed by the users private key. The signature is verified with the users public key and the user is granted or denied access.

### **ENCRYPTED DATA GATEWAY ENGINE (EDGE)**

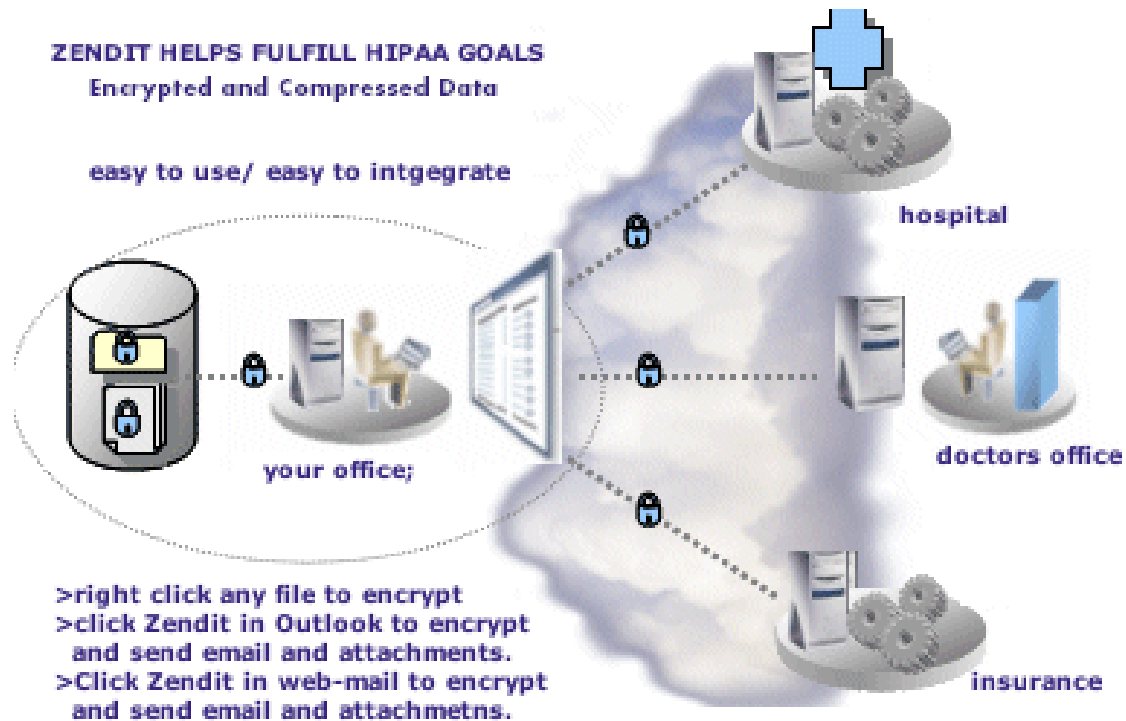
EDGE is an electronic data-armoring device that performs all cryptographic functions (encryption, decryption, digital signing and authentications) for the Zendit Public Key Framework according to administrators centrally configured data security policies for an entire organization.. The encrypted data gateway works in conjunction with the enterprise Sovereign Server and the Each deployment of the EDGE can process from 10,000 to 1 million cryptographic functions a day.

### **TRUST AGENTS:**

Zendit technology combines one-click encryption™ solution with hybrid client/server and peer-to-peer encryption/authentication services. **Our Client Plugins are basically “encryption control” enhancement for Mainstream browsers, mail clients desktops and operating systems. They work in conjunction with our Zendit’s Enterprise Sovereign Servers and Trustpoints which in turn facilitates seamless Public Key Exchange, Management, and Authentication.** This intelligent architecture brings elegance and seamlessness to the infamous pain end users have faced when it comes to using Public key cryptography. By this we mean--no more painful installation of certificates or hunting down public keys or facing recipients who are not encryption enabled and are fearful of the technology.

Zendit’s innovative, suite of web security, encryption, digital signature, privacy and anti-fraud tools serve end users with the ability to easily secure/encrypt (without breaking standard security models) their online communications, digitally sign their transactions, manage their online identities, and grants access to our seamless public key framework. The growing suite of Zendit clients includes Browser, Web page, Outlook, Desktop, and in the near future Macintosh, Java, Windows CE and Palm. Trust Clients are installed on user computers.

The system solves a barrier to the standardization of encryption: The inability to send encrypted data to non-encryption enabled users. The system “encryption-enables” first time recipients and generates Locks (public keys) which can serve as an electronic version of a signature card and can evolve into a REAL online passport—(REAL because the foundation of the passport is user controlled cryptography) and Private Keys for decryption and digital signatures (electronic version of what will evolve into a legally binding signature) . Details of our clients follow:



**ZENDIT SURFBOARD** –Simple to use/intuitive client *The Zendit Surfboard* is a secure toolbar that pops into the users browser and offers "one click encryption", decryption , digital signing, and verification of HTML and XML web-forms and web-mail systems, The system is able to support estimated 170 million web-based email users (including hotmail and yahoo!) and the estimated 44.2 million Exchange/Outlook users. In addition the system can support an unlimited number of customized web-forms.

- **WEB PAGE** – Browser Initiated Zendit (BIZ) allows customized web pages to initiate the encrypt, sign, decrypt and verify functions seamlessly without the need of selecting an additional button. All encryption and decryption still happens on the client.
- **OUTLOOK** – The Outlook Trust Client allows the encryption, signing, decryption and verifying functions in the easy to use Outlook email interface. The Outlook Trust Client can be configured to automatically encrypt and sign all outbound mail without a change in the user experience.
- **DESKTOP** – Currently the Desktop Trust Client is available for Windows 95, 98, XP, and ME, NT, 2000. It allows the encryption and decryption of files locally on a computer.
- **WEBVAULT & LOCAL VAULT** - The system offers intuitive Lock and Key management. Travel Mode enables users to store their private key in their web vault so they can access and manage their key from any computer.
- **SEAMLESS KEY EXCHANGE AND VERIFICATION** - Facilitating seamless Public Key (Lock) Management and Authentication.
- **WEB ID AND WEB ENTRY**-- With Web ID WebEntry: The system allows users to generate multiple key pairs and associate them as identities for different verification purposes online, for instance one website may to need only know that

the user is over 18 and nothing else, another may need home address and credit card number and another may need social security number , etc. The system again offers real world authentication processes which reduces the privacy dangers of using any identifier consistently, privacy is protected without sacrificing security. The key holder has control over what information is disclosed, and to whom.

## **How Authora's Solutions Map to the Privacy Rule and Forthcoming Security Standard**

### ***Privacy Rule Requirements General Prohibition § 164.502(a)***

**Explanation of Requirement:** HIPAA prohibits all disclosures of PHI, except as expressly permitted. This legal approach makes compliance difficult because it requires a covered entity to consider most situations in advance and implement a policy and/or procedure to address it.

#### **How Authora addresses this requirement:**

The Authora Sovereign Server works in concert with Authora's Trust Points and EDGE Server to allow organizations to scan outgoing messages and attachments for PHI and protect this content automatically in accordance with established corporate policies. Information is encrypted so that it is secure during delivery to another system or recipient, or when stored on a network.. In addition, authorized groups or individual recipients must Authenticate themselves to receive the information.

### ***Minimum Necessary Standard § 164.502(b); 164.514(d)***

**Explanation of Requirement:** When using, disclosing or requesting PHI from a covered entity, the entity must make reasonable efforts to limit the information to only the minimum necessary needed to accomplish intended purposes. These measures include: identifying individuals or classes of individuals who need access to PHI, establishing categories of PHI that are needed, and limiting access to information accordingly.

**How Authora addresses this requirement:** Authora's patent pending Sovereign Platform technology lets covered entities strictly control PHI to facilitate adherence to the Minimum Necessary Standard. Authora provides:

- **User based access:** access to PHI can be limited to specific individuals or groups Role-based access: achieved by tying roles to group memberships
- **Content-based access:** determined from another application and communicated to content protected by Authora applications via Authora's external authorization API.

Authora's products can also be used to control how recipients use PHI after they receive it including: How long recipients can view it and which systems or entities can view the information.

**Below are key security attributes of Authora's product suite that address these HIPAA requirements.**

**Encryption** – Transforming confidential plaintext into cipher text to protect it.

**How Authora addresses this requirement:** Authora encrypts content using industry Standard cryptographic techniques with 128-bit keys. Unlike other encryption systems that

routinely pass copies of the keys with the protected information, Authora's products always store keys separate from the protected content. This provides a higher level of information security.

**Authentication (Entity)** – The corroboration that an entity is the one claimed

**How Authora addresses this requirement:** Authora's product suite implements a wide range of standard user Authentication methods to prove the identity of users before they access information. Authentication methods range from a username and password to NT and Public Keys .

**Authoration (Data)** – The corroboration that data has not been altered or destroyed in an unauthorized manner

**How Authora addresses this requirement:** When content is encrypted, the resulting protected data is validated using the generally accepted RSA MD5 hash. Authora's client applications will recognize and report any changes in file content and refuse to open if the hash values do not match those recorded at the time of data registration. This process ensures the integrity of confidential data.

**Access/Authorization Controls** – Mechanisms for obtaining consent for the use and disclosure of health information.

**How Authora addresses this requirement:** Authora's product suite ensures that only authorized individuals can view information and that information is properly controlled. Information policies can be established that control who can view information, when it can be viewed and whether recipients have the rights to forward, copy/paste, or print information. These permissions can be changed at any time, even after recipients access information.

**Audit Controls** – Mechanisms employed to record and examine system activity.

**How Authora addresses this requirement:** Authora can provide a detailed audit trail provides proof that information has been accessed appropriately. Every access to and use of information is recorded, including when information is viewed or printed and by whom.

## **Conclusion:**

As automation of transactions and regulatory protection of the data continues to evolve, cryptography becomes the foundational security control tool for organizations. Secure e-mail, access control; e-commerce, extranets, web services, and other applications for online business require a strong yet simple to implement cryptographic security architecture. Authora has developed a robust Public Key Framework for regulatory compliance that eases integration, management, and simplifies the use of public key cryptography for both the enterprise and the average net user. At Authora we believe in the future every network and every net user will be encryption-enabled. By "encryption-enabled" we mean in control of cryptographic functions, in control over access and authentication policies, in control of cryptographic keys, in control of our many different online identities and relationships, and in control of the confidentiality of digital assets.

Now more than ever encrypting data and understanding the context of the data--via digital signatures—has become a significant business need. Zendit solutions answers this escalating need with a robust, scalable public-key framework with complementary public-key enabled applications that “trust-enable” existing servers and applications residing on networks and users machines outside the network such as remote employees, vendors and consumers. By “trust-enable” we mean crypto/public key-enabled net users and networks.