

Secure Electronic Communications Under HIPAA: Issues and Answers

ZIXCORP | AUGUST 2004



INSIDE:

- > HIPAA Compliance: Solving the Email Problem
- > Who Must Comply with HIPAA
- > HIPAA Penalties and Enforcement
- > The HIPAA Compliance Schedule
- > The Privacy Rule and the Security Rule

Table of Contents

| | |
|--|-----------|
| 1.0 INTRODUCTION: THE PURPOSE OF THIS WHITE PAPER..... | 1 |
| 1.1 HIPAA Compliance: Solving the Email Problem | 1 |
| 1.2 Organization of the White Paper | 1 |
| 2.0 WHAT IS HIPAA?..... | 2 |
| 2.1 Who Must Comply with HIPAA? | 2 |
| 2.1.1 The HIPAA Business Associate Problem, and Its Solution | 3 |
| 2.2 HIPAA Penalties and Enforcement | 4 |
| 2.2.1 Avoiding or Defending Against HIPAA Penalties | 4 |
| 2.3 The HIPAA Compliance Schedule..... | 4 |
| 2.4 The Privacy Rule and The Security Rule..... | 5 |
| 2.5 The HIPAA Security Rule | 6 |
| 2.5.1 Risk Analysis and Management: the Foundation of the Security Rule. | 7 |
| 2.5.2 Making Decisions About Required Specifications | 7 |
| 2.5.3 Making Decisions About Addressable Specifications | 8 |
| 2.5.4 Standards and Specifications Under the Security Rule..... | 9 |
| 3.0 RISKS AND HIPAA..... | 11 |
| 4.0 HIPAA COMPLIANCE AND ZIXCORP..... | 13 |
| 4.1 ZixCorp Solutions and HIPAA Requirements | 13 |
| 4.1.1 ZixSecure Center™..... | 14 |
| 4.1.2 ZixMail® Desktop Email | 15 |
| 4.1.3 ZixVPM® (Virtual Private Messenger)..... | 15 |
| 4.1.4 ZixMessage Center™..... | 15 |
| 4.1.5 ZixAuditor® | 15 |
| 4.1.6 ZixCorp User Awareness Program™..... | 16 |

1.0 INTRODUCTION: THE PURPOSE OF THIS WHITE PAPER

The purpose of this white paper is to explain the role ZixCorp's secure e-messaging solutions can play in helping healthcare organizations comply with the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The intent is to describe a specific problem and its solution while avoiding hype on the one hand, and fear, uncertainty and doubt (FUD) on the other.

1.1 HIPAA Compliance: Solving the Email Problem

HIPAA compliance is a complex task and no technology services vendor can provide a total solution. However, the right kinds of services can solve specific compliance problems, and competent vendors can appropriately assume some of the burdens of HIPAA compliance.

The specific problem this white paper will address is the HIPAA-compliant use of email. HIPAA does not prohibit the use of the Internet or email, but does require those individuals and organizations it regulates to assess the risks to information their activities pose, and take steps to reduce or eliminate those risks.

Internet email poses well-known risks that unauthorized individuals will intercept or retrieve messages. HIPAA compliance therefore requires Internet email to include mechanisms and services that prevent unauthorized interception or receipt of email. In almost all cases these requirements will call for encryption of email messages, and for procedures that authenticate the identity of the recipients of such messages.

ZixCorp provides a number of services that fulfill these requirements. The full set of services offered by ZixCorp covers all Internet email HIPAA compliance needs, from risk assessment through encryption and authentication, to compliance auditing, and user training. These services are provided through communications and services facilities including the ZixSecure Center™, which is constructed and operated in accordance with the strictest security standards.

The use of ZixCorp's secure e-messaging solutions and related services therefore addresses and solves HIPAA compliance problems arising from the use of Internet email. This may not solve all of an organization's HIPAA compliance problems, but ZixCorp can usefully assume the burden of compliance in this specific, important area.

1.2 Organization of the White Paper

This white paper is organized to cut through some of the confusion and FUD that is all too frequently encountered in discussions of HIPAA compliance. The first section is a summary of HIPAA itself, intended to clarify what "HIPAA compliance" really means, and how it should be approached. The second section is a discussion of email

risks and what they mean to HIPAA compliance, and the third section will specifically show how ZixCorp's applications and services may be used and satisfy requirements for HIPAA compliance.

2.0 WHAT IS HIPAA?

HIPAA stands for the "Health Insurance Portability and Accountability Act of 1996." HIPAA itself is a long, complex law that covers a number of important areas in the regulation of healthcare, from the portability of healthcare benefits and claims fraud and abuse penalties, to electronic health benefits claims processing and beyond. As a result, there has been some confusion about what HIPAA really means and does.

One of the most important things HIPAA has done is to create unprecedented regulations for the privacy of information about individuals, and the security of information systems used by healthcare professionals and organizations. While HIPAA became law in 1996, these privacy and security regulations (the "Privacy Rule" and the "Security Rule") were issued later by the United States Department of Health and Human Services (HHS) on a phased-in basis. The relationship between these rules and their compliance schedules will be discussed below.

2.1 Who Must Comply with HIPAA?

It is important to understand that HIPAA is not a universal privacy or security law. This means that it does not apply to everyone, but only to certain kinds of organizations and individuals involved in healthcare. These organizations and individuals are called "Covered Entities" under HIPAA. Covered Entities include healthcare providers, health plans, and certain kinds of health benefits claims processing companies called "healthcare clearinghouses."

HIPAA may not apply to everyone, but it does apply to almost all organizations and individuals in the healthcare sector. Healthcare providers as Covered Entities include any individual or organization which is paid for providing healthcare, from individual physicians and nurses through hospitals, health maintenance organizations (HMOs), clinical laboratories, long-term care facilities, and so on. Health plans include any organization that pays the cost of healthcare for others, excepting only life and accident insurance payments. The law applies equally to for-profit and nonprofit organizations, and governmental as well as private entities.

Because HIPAA is not a universal law, it also does not apply to all personal information. Rather, it applies to "Protected Health Information," sometimes also referred to as "PHI." Protected Health Information is any information that identifies or could be used to identify an individual and has anything to do with past, present or future physical or mental health conditions, care or payment for care.

This is a very broad definition and includes almost all information about individuals a Covered Entity may create, collect or possess. Covered Entities will be required to manage and protect the Protected Health Information in their possession or control according to the requirements of the Privacy and Security Rules.

2.1.1 THE HIPAA BUSINESS ASSOCIATE PROBLEM, AND ITS SOLUTION

Because HIPAA is not a universal privacy law, HHS does not have the legal authority to directly regulate individuals or organizations that are not in the Covered Entity category. However, Covered Entities have many legitimate needs to make Protected Health Information available to non-Covered Entities, such as technology services providers, consultants, lawyers, and so on. Under HIPAA, these kinds of parties are called “Business Associates.” The fact that Covered Entities have many legitimate needs to share Protected Health Information with Business Associates that are not covered by HIPAA creates a problem with Business Associates.

The provision of Protected Health Information to a party that is not a Covered Entity could create a serious loophole in HIPAA’s protections. Since HHS does not have the authority to directly regulate a party that is not a Covered Entity, that party could, in theory, use or distribute Protected Health Information in ways prohibited by HIPAA. If this loophole were not closed, Covered Entities could use Business Associates to remove Protected Health Information from the protection of HIPAA, and thus escape or avoid compliance.

HHS realized that it would not be practical to try to prohibit Covered Entities from using Business Associates, since they perform too many essential or useful services. HHS therefore solved the Business Associate problem by the creation of the “Business Associate Contract.”

The Privacy and Security Rules explicitly allow a Covered Entity to provide or disclose Protected Health Information to any person who “performs, or assists in the performance of [any] function or activity involving the use or disclosure of ‘Protected Health Information’ on behalf of” the Covered Entity. In order to solve the Business Associate problem, these rules require the Covered Entity to first establish “satisfactory assurance that the Business Associate will appropriately safeguard the information.”

This required “satisfactory assurance” may only be met by “a written contract or other written agreement or arrangement with the Business Associate” that includes a number of required provisions. A contract including these provisions is called a Business Associate Contract. The solution to the Business Associate problem, then, is the Business Associate Contract.

2.2 HIPAA Penalties and Enforcement

One of the major concerns in HIPAA compliance is the criminal penalty provision of the law. HIPAA is the first federal law to impose criminal penalties for an improper use or disclosure of personal information, in this case Protected Health Information. These penalties range from one year in prison and a five thousand dollar fine for simply violating the law, up to ten years in prison and a two hundred fifty-thousand dollar fine for violating the law with malice or for profit.

Civil penalties are also available, and may be imposed upon any Covered Entity that fails to comply with the requirements of any of the HIPAA regulations. Civil penalties range up to twenty-five thousand dollars per year for any given type of violation.

The Office of Civil Rights (OCR) of HHS will investigate civil violations and will impose any civil penalties. Criminal violations will be investigated and prosecuted by the United States Department of Justice and the Federal Bureau of Investigation.

2.2.1 AVOIDING OR DEFENDING AGAINST HIPAA PENALTIES

In order to impose either civil or criminal penalties for a violation of HIPAA, there must be proof that the party charged failed to comply with a requirement of the HIPAA legislation or one of the regulations. A criminal conviction for improper use or disclosure of Protected Health Information will only be possible with proof that the use or disclosure somehow arose from or was connected to such a violation.

Unfortunately, there is no “safe harbor” for HIPAA compliance. Each Covered Entity must make its own compliance choices under both the Privacy and the Security Rules; both rules are “scalable,” meaning that the protections each Covered Entity implements must be “those appropriate to its specific needs, risks, and environments.” Such a flexible approach is probably unavoidable, since the rules have to apply to such a wide range of organizations. In practice, this standard means that almost all HIPAA compliance solutions are up to each Covered Entity’s prudent, informed choice.

The best defense against either a civil or a criminal violation claim will therefore be an organized HIPAA compliance program, which makes sensible, documented decisions about compliance with each of the requirements of the Privacy and Security Rules.

2.3 The HIPAA Compliance Schedule

HHS issued a proposed draft of the Security Rule in August 1998, and the final rule was published on February 20, 2003. Compliance with the Security Rule will be required no later than April 21, 2005 for most Covered Entities.

The final Privacy Rule was published in December 2000, after an initial draft published in November 1999. A set of amendments to the Privacy Rule was published in August 2002. Compliance with the final rule, as published in December 2000 and amended in August 2002, is required as of April 14, 2003 for most Covered Entities.

Congress passed legislation extending the HIPAA compliance date for a set of regulations that have not been discussed here: the "Transactions Rule." The Transactions Rule specifies the required electronic formats and codes for a number of healthcare claims transactions, like checking an individual's eligibility for coverage, or a physician practice submitting a claim for payment to a health plan. Compliance with the Transactions Rule was originally scheduled for October 2002, but Congress passed the Administrative Simplification Compliance Act (ASCA) that allowed Covered Entities to obtain a compliance extension until October 2003. Congress made it clear that ASCA does not apply to any other HIPAA rules, including the Privacy Rule.

Covered Entities should try to bring themselves into compliance with the Security Rule as much as possible, even before compliance is technically required, since HIPAA is likely to set general standards of care before then. This has already happened in one federal court case, United States v. Sutherland, where the court noted:

Although the Standards [*i.e.*, the Privacy Rule] were effective April 14, 2001, compliance is not required until April 14, 2003. ...Nevertheless, the Standards indicate a strong federal policy to protect the privacy of patient medical records, and they provide guidance to the present case.... Although not presently binding on the Hospital or this court, I find these regulations to be persuasive in that they demonstrate a strong federal policy of protection for patient medical records....

2.4 The Privacy Rule and The Security Rule

It would also be prudent to take the Security Rule into account in establishing information "safeguards" required by the Privacy Rule. As discussed above, the Privacy Rule is effective as of April 2003 while the Security Rule will not become effective until April 2005. However, the line between "Privacy" and "Security" is not clear. The privacy of information cannot be assured without safeguards that secure it against disclosure to unauthorized parties.

Because security is a necessary part of privacy, the Privacy Rule includes a requirement that all Covered Entities implement "appropriate administrative, technical, and physical safeguards to protect the privacy of Protected Health Information." These safeguards, like all the Privacy Rule provisions, are effective as of April 2003. The term "safeguard" in the Privacy Rule is therefore a

requirement that Covered Entities establish appropriate security for Protected Health Information, though it does not spell out specific details.

HHS expressly discussed the value of using the Security Rule as guidance for Privacy Rule compliance in the Preamble to the Security Rule (emphasis added):

[S]ecurity and privacy are inextricably linked. The protection of the privacy of information depends in large part on the existence of security measures to protect that information.

As a result, a safeguard adopted for compliance with the Privacy Rule may well be appropriate for compliance with the Security Rule as well:

[It] is likely that Covered Entities will meet a number of the requirements in the security standards [i.e., Security Rule] through the implementation of the privacy requirements. . . . *E-mail authentication procedures put into place for privacy protection may also meet the security standards, therefore eliminating the needs for additional investments to meet these standards.* As a result, Covered Entities that have moved forward in implementing the privacy standards [i.e., Privacy Rule] are also implementing security measures at the same time.

Conversely, of course, a compliance solution that would be appropriate under the Security Rule will be considered appropriate for Privacy Rule compliance purposes. Therefore, while compliance will not technically be required until 2005, the Security Rule is very persuasive guidance as to what “safeguards” are appropriate under the Privacy Rule.

For this reason, Covered Entities should follow the guidance of the Security Rule in complying with the “safeguards” requirement of the Privacy Rule. A Covered Entity that does not follow the guidance of the Security Rule, might face a situation where there is an improper disclosure of Protected Health Information, which could have been avoided by complying with the Security Rule. This could lead to a civil enforcement action or even criminal charges based on the failure to implement appropriate “safeguards.”

2.5 The HIPAA Security Rule

The Security Rule requires Covered Entities to use a **Risk Assessment**-based approach to decide on appropriate safeguards for implementation of four broad categories, including:

- **Organizational Requirements** for the corporate or other organizational relationships among subdivisions of entities performing functions covered by HIPAA, and for documentation of policies and procedures.

- **Administrative Procedures** for the management of personnel, facilities and equipment involved with information systems or electronic media.
- **Physical Safeguards** for the protection of computer equipment, workstations, and network connections.
- **Technical Safeguards** for the protection of Protected Health Information stored or transmitted in information systems and electronic media.

Each of these categories is divided into a number of required elements, as discussed in more detail below.

2.5.1 RISK ANALYSIS AND MANAGEMENT: THE FOUNDATION OF THE SECURITY RULE

The Security Rule is organized in a somewhat distinctive way. The regulations distinguish between “standards” and “implementation specifications,” and give Covered Entities a fairly high degree of discretion in deciding what specific security measures they will adopt. However, this discretion comes at a price.

The rule does not give Covered Entities the comfort of “safe harbors” that is, it does not provide detailed compliance instructions, but requires Covered Entities to make reasoned, informed, and documented risk management decisions which justify the security measures they choose to adopt. As stated in the Preamble to the Security Rule, “[a Covered Entity] must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks and vulnerabilities.”

Each Security Rule standard, therefore, identifies a kind of safeguard that addresses information risks and vulnerabilities. The specifications then identify the “effective steps” needed to manage those risks and vulnerabilities.

- “The security standards . . . define administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information.”
- “The implementation specifications . . . provide instructions for implementing those standards.”

Some standards include their own implementation specifications – that is, reading the standard itself should provide sufficient information to allow a Covered Entity to determine what “effective steps” it should take to meet the standard. Instructions for compliance with the other standards are given in either “required” or “addressable” specifications, which are published along with their standards.

2.5.2 MAKING DECISIONS ABOUT REQUIRED SPECIFICATIONS

Compliance with specifications that are included in their standard is mandatory, as is compliance with “required” specifications. In deciding exactly which

security measures it should adopt to comply with a required specification, a Covered Entity is required to use a “flexible approach” that selects specific security measures based on the following factors:

- “The size, complexity and capabilities of the Covered Entity.”
- “The Covered Entity’s technical infrastructure, hardware and software security capabilities.”
- “The costs of security measures.”
- “The probability and criticality of potential risks to electronic protected health information.”

2.5.3 MAKING DECISIONS ABOUT ADDRESSABLE SPECIFICATIONS

“Addressable” specifications are intended to give Covered Entities an additional degree of flexibility in meeting certain standards. While required specifications and those included in standards must be followed, in making security decisions under an “addressable specification” a Covered Entity may choose an alternative approach. The following rules apply to decisions about compliance with addressable specifications:

- The first step is to assess whether the specification “is a reasonable and appropriate safeguard” for the protection of information, in the Covered Entity’s “environment.”
- If the Covered Entity finds that the specification is “reasonable and appropriate,” it should implement it. The specific means by which the specification is implemented is chosen by use of the “flexible approach,” using the same factors applicable to required specifications.
- If the Covered Entity finds that the specification does not apply to its “environment” – that is, if the security risks addressed by the standard simply do not exist because of the way it operates or its systems are organized – it need not implement either the specification or any alternative. If the Covered Entity chooses this alternative, it must “document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met.”
- If the Covered Entity finds that the specification is not “reasonable and appropriate,” but that some alternative approach works better (i.e., is “more reasonable and appropriate”) it may adopt the alternative solution. As with a decision that a specification is not applicable, the decision to adopt an alternative and the reasoning behind it must be documented.

Both “flexible approach” and “addressable specifications” decisions are based on the same types of factors, and these factors must be identified through a risk assessment. Instead of the comfort of “safe harbors” the Security Rule requires a

structured, informed and documented decision-making process leading to the selection of “reasonable and appropriate” safeguards.

2.5.4 STANDARDS AND SPECIFICATIONS UNDER THE SECURITY RULE

The Security Rule standards and specifications fall into the following general categories. Each standard should be reviewed as a general type of safeguard that addresses risks to and vulnerabilities of Protected Health Information, which are to be managed according to its specifications.

The ***Organizational Requirements*** standards and specifications are the following:

- The *Healthcare Component* standard is implemented by the ***required*** operational separation of components of organizations that perform activities regulated by HIPAA from those that do not.
- The *Affiliated Covered Entity* standard applies to organizations that are legally affiliated with one another and wish to comply with HIPAA as an integrated group, and is ***required*** to be implemented by documenting their relationship and managing the group under consistent policies and procedures.
- The *Business Associate Contract* standard is ***required*** to be met by entering into a Business Associate Contract or other appropriate documentation including a requirement of “safeguards,” with any party that creates or obtains Protected Health Information on behalf of a Covered Entity.
- The *Policies and Procedures* and *Documentation* standards ***require*** the adoption of policies and procedures used for Security Rule compliance in writing, and retention of those policies, procedures and records of all relevant compliance decisions for at least six years from their last effective date.

The ***Administrative Procedures*** standards and their specifications include the following:

- A *Security Management Process* standard which is ***required*** to be implemented by conducting a risk analysis, implementing risk management and a sanction policy, and procedures for regular information system activity review.
- The *Assigned Security Responsibility* standard ***requires*** identification of a responsible security official.
- The *Workforce Security* standard is met by ***addressable*** specifications for authorization and/or supervision of workforce members working with Protected Health Information, and workforce security clearance and termination procedures.

- The *Information Access Management* standard is implemented by **required** isolation of any healthcare clearinghouse functions, and **addressable** specifications for information access authorization, establishment, and modification.
- The *Security Awareness* standard is met by **addressable** specifications for security reminders, protections against malicious software (e.g., computer viruses), log-in monitoring, and password management.
- The *Security Incident Response* is **required** to be met by policies and procedures for identifying, responding to, and documenting security incidents.
- The *Contingency Plan* standard is met by **required** data backup, disaster recovery, and emergency mode operations plans, and **addressable** plan testing and revision procedures and applications and data criticality analysis.
- The *Evaluation* standard **requires** an evaluation of how well security policies and procedures comply with the Security Rule's requirements, both periodically and whenever there are material changes in operations or the security environment.

Standards and specifications in the ***Physical Safeguards*** category include:

- A *Facility Access Controls* standard implemented by **addressable** specifications for contingency facility access, and facility security plans, access controls and maintenance records.
- *Workstation Use* and *Workstation Security* standards which **require** policies and procedures specifying the proper functions and physical configuration of computer workstations used to access Protected Health Information, and physical safeguards restricting workstation access to authorized users.
- A *Device and Media Controls* standard implemented by **addressable** specifications for the disposal and re-use of computers and other devices and electronic media (e.g. floppy disks or CD-ROMs) used with Protected Health Information, for tracking their physical movements and individuals responsible for them, and for data backup and storage.

The ***Technical Safeguards*** standards and specifications required for the protection of information systems and stored data include:

- An *Access Control* standard implemented by specifications that **require** unique information system user names and/or numbers and emergency information access, and by addressable specifications for automatic system logoff, and encryption and decryption of stored information.

- *Audit Controls*, a standard **required** to be implemented by hardware, software or procedures for the review of information system activity.
- Integrity standard, implemented by an addressable specification for authentication to ensure data has not been altered or destroyed without authorization.
- *A Person or Entity Authentication* standard **requiring** procedures for verifying the identity of parties seeking access to electronic Protected Health Information.
- *A Transmission Security* standard, implemented by **addressable** specifications for integrity controls to ensure that transmitted information is not improperly modified without detection, and for encryption “whenever deemed appropriate.”

3.0 RISKS AND HIPAA

Electronic mail, familiarly known as email, poses two basic and well-known security risks: Unauthorized interception of messages in transmission, and receipt of messages by unauthorized persons. These are unavoidable risks, which arise (for reasons beyond the scope of this white paper) from the technology of the Internet itself.

The fact that these risks exist does not mean that the Internet cannot be used for the transmission of messages including Protected Health Information, but as with all other areas of HIPAA Privacy and Security Rule compliance, it does mean that “reasonable and appropriate safeguards” must be used.

These risks are addressed by two of the Technical Safeguards standards in the Security Rule: “Person or Entity Authentication,” and “Transmission Security.” The former standard requires implementation of procedures that verify the identity of parties seeking access to Protected Health Information. A Covered Entity using email to transmit Protected Health Information therefore must implement some mechanism that confirms the identity of the recipient before he or she has access to the email.

The Transmission Security standard is implemented by addressable specifications for data integrity controls and encryption. As discussed above, the fact that these specifications are “addressable” does not mean that they are optional. Rather, it means that they must be implemented unless an informed, reasoned, and documented risk analysis demonstrates that they are not “reasonable and appropriate,” and alternative safeguards which address the same risks and vulnerabilities in a “more reasonable and appropriate” fashion are adopted instead.

How these specifications are met therefore depends on the technologies used for electronic transmissions. In discussing this standard in the Preamble to the

Security Rule HHS noted that some transmission technologies present a low risk of security violation:

A significant number of comments were received on the question of encryption requirements when dial-up lines were to be employed as a means of connectivity. The overwhelming majority strongly urged that encryption not be mandatory when using any transmission media other than the Internet[.] . . . Many comments noted that there are very few known braches of security over dial-up lines . . .

...

We agree with the commenters that switched, point-to-point connections, for example, dial-up lines, have a very small probability of interception.

Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines.

It is not clear what sources HHS used to determine what encryption technologies might be available, and their possible costs and burdens, in deciding that encryption would be encouraged but not required for other types of transmissions:

We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting email communications with patients. [sic] As a result, we decided to make encryption in the transmission process an addressable specification. Covered Entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the Internet.

Even so, the decision not to use encryption must be informed by a risk analysis, and appropriate to the risks potentially involved.

As business practices and technology change, there may arise situation where electronic protected health information being transmitted from a Covered Entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis showed such risk to be significant, we would expect Covered Entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption.

The decision-making process for use of encryption for Internet email under the Security Rule would therefore have the following steps:

- A risk analysis which identified the potential for unauthorized access to email, either in transmission or when received at the addressee's email account. This risk analysis would consider the frequency and volume of anticipated email, whether or not there was a risk that unauthorized parties would target email from the Covered Entity for interception (e.g., if the emails routinely contained information valuable for purposes of identity theft), and the risk that unauthorized parties might have access to addressee's email accounts (e.g., shared family or office accounts, email received at a work account to which an employer would have access).
- An analysis whether or not reasonably available encryption solutions might provide an appropriate safeguard against identified risks, at a reasonable cost and operational burden. If it is determined that such solutions are available, one should be adopted and the analysis ends.
- If it is determined that there is no reasonable and appropriate encryption solution available, the next step would be an analysis of available alternatives which would address the same risks better given the operational environment. For a Covered Entity that had little operational need or desire to use Internet email, an appropriate decision might be to prohibit or severely limit its use as a matter of policy. Otherwise, some safeguard which addresses the same risks at a more reasonable cost and burden and/or in a more appropriate way than encryption must be adopted.

The same analytic steps would then have to be followed for the data integrity controls specification under the Transmission Security standard.

4.0 HIPAA COMPLIANCE AND ZIXCORP

ZixCorp provides a number of products and services that Covered Entities can use to ensure their compliance with HIPAA while using Internet email. These solutions meet the Security Rule requirements, and include other features that support HIPAA compliance by Covered Entities.

While ZixCorp is not a Covered Entity, it holds itself to a level of compliance with HIPAA's requirements "scaled" to the largest, most technologically capable healthcare organizations. ZixCorp's solutions are therefore appropriate email related "safeguards" for any size or type of Covered Entity.

4.1 ZixCorp Solutions and HIPAA Requirements

While ZixCorp cannot take on all of a Covered Entity's HIPAA compliance burdens, it can relieve much of the burden of managing HIPAA security on the

Internet. Covered Entities have a choice of solutions which they can integrate into their own compliance programs as they find appropriate. In each case, ZixCorp manages the HIPAA compliance requirements applicable to its responsibilities to the same standards a prudent, capable Covered Entity would follow.

The core of ZixCorp's suite of solutions is the management and distribution of "encryption keys," the data sets and algorithms used to encrypt and decrypt messages. This technology implements a solution meeting both specifications under the Security Rule Transmission Security standard; it not only encrypts, but also provides a data integrity control methodology. And because email addressees are not provided with the keys needed to decrypt messages until they have verified their identities, this technology also implements a solution meeting the required specification for the Person or Entity Authentication standard.

ZixCorp, therefore, provides a complete set of safeguards addressing the standards and specifications applicable to email. Other ZixCorp products and services complement these safeguards; the specific applications of the HIPAA Security Rule requirements to ZixCorp's various solutions are as follows:

4.1.1 ZIXSECURE CENTER™

The keystone of the security architectures provided by ZixCorp's secure messaging solutions is the SysTrust™ and SAS-70-certified ZixSecure Center, which ensures secure delivery of electronic messages. The Center is designed to support uninterrupted operations and has the capacity, scalability, and infrastructure to support encryption keys for every email address in the world.

The ZixSecure Center maintains redundant hardware and network functionality for all critical systems. The facility has multiple electrical feeds from independent utility power grids, dual uninterruptible power supplies, a backup diesel generator, and redundantly configured power distribution units. Internet connections are maintained through three ISPs, using two independent, expandable Fiber rings at rates of up to OC-12.

The ZixSecure Center is staffed 24-hours a day with trained personnel constantly monitoring the facilities, networks, systems and applications. All personnel in critical or sensitive positions have been subject to background checks and security clearance procedures and policies appropriate to their responsibilities and systems access privileges. Appropriate incident response and contingency plans and policies are in place, and the security of the ZixSecure Center is assessed on a routine basis.

The ZixSecure Center meets or exceeds all standards for ***Physical*** and ***Technical Safeguards*** that would apply to a sophisticated, highly competent Covered Entity's comparable facilities under the Security Rule. It is also administered consistently with the ***Administrative Safeguards*** that meet or exceed those that would be applicable to any Covered Entity managing the same type of operations.

4.1.2 ZIXMAIL[®] DESKTOP EMAIL

ZixMail is a desktop secure e-messaging solution. ZixMail meets the requirements for *Technical Safeguards* for Internet messaging under the Security Rule by providing strong encryption and data integrity controls, coupled with strong access controls through the use of unique user names and passphrases. ZixMail also provides time-stamping and the ability to archive encrypted messages. It also meets the need to confirm and authenticate message content.

4.1.3 ZIXVPM[®] (VIRTUAL PRIVATE MESSENGER)

Like ZixMail, ZixVPM provides *Technical Safeguards* appropriate for compliance with the HIPAA Security Rule, but supports more sophisticated management of Internet messaging by providing encryption company-wide. As a sure stopgap to PHI leaks, ZixVPM includes a pre-configured HIPAA lexicon that automatically detects and encrypts all email messages containing PHI. This automatic content recognition program eliminates human error and reliably prevents disclosures.

ZixVPM provides the same strong encryption, data integrity and access controls as ZixMail, but enables customers to set and enforce organization-specific policies for secure Internet usage. This permits organizations greater flexibility and customization in managing their secure messaging while still maintaining HIPAA compliance.

4.1.4 ZIXMESSAGE CENTER[™]

The ZixMessage Center is a secure Web-based portal that provides a browser-based solution for sending and receiving secure messages over an encrypted Secure Sockets Layer (SSL) Internet connection. This service enables ZixMail and ZixVPM subscribers to send encrypted messages to non-ZixCorp users without requiring the recipient to subscribe to ZixCorp services or buy or use any specialized encryption software.

Messages are stored in the ZixSecure Center[™] until their expiration date or until the recipient opens and deletes the message, whichever comes first. The ZixMessage Center generates and sends pickup receipts and expiration notices to the sender, and replies with the Best Method of Delivery[™].

Because the ZixMessage Center is managed as part of the ZixSecure Center, this service meets or exceeds the Security Rule compliance standards that would apply to Covered Entities performing the same functions for themselves.

4.1.5 ZIXAUDITOR[®]

ZixAuditor is a *Risk Assessment* tool for email that determines the extent to which Protected Health Information, or other sensitive or confidential information, is being

transmitted without appropriate safeguards. Once secure messaging policies have been developed and a secure messaging solution has been implemented, ZixAuditor serves as the internal auditing application necessary to meet the *Evaluation* standard of the Security Rule.

4.1.6 ZIXCORP USER AWARENESS PROGRAM™

The *Security Awareness* standard calls for training and awareness materials as a part of Security Rule compliance. The ZixCorp User Awareness Program includes training materials designed to help users become aware of the risks of unsecured Internet messaging, and how to use the customer's ZixCorp solutions to avoid them.

For more information about ZixCorp's suite of solutions for HIPAA compliance, please call (866) 257-4949, visit www.zixcorp.com, or email sales@zixcorp.com.



2711 N. Haskell Ave.
Suite 2300, LB 36
Dallas, TX 75204
1-866-257-4949
www.zixcorp.com