

Essential Security Software™ presents:

# Securing Healthcare Information with eCipher™

**Table of Contents**

**Contents**

Securing Healthcare with ECipher™ : Overview ..... 2

Health Insurance Portability and Accountability Act (HIPAA)..... 3

Penalties for HIPAA Violations ..... 3

Common HIPAA Scenario Crises and the eCipher Solution ..... 3

On-line Pharmaceutical Providers ..... 4

Healthcare Providers to Communicate with Patients via Email ..... 4

ECipher: Facilitating HIPAA Compliance ..... 6

eCipher Features and Benefits..... 7

Decreasing Your Vulnerabilities ..... 7

Summary ..... 7

Evaluate eCipher for Free ..... 8

Our Commitment: “The Customer Comes First” ..... 8

**Securing Healthcare with ECipher™ : Overview**

Protecting patient privacy is an important issue in the medical profession. New laws are being enacted, requiring medical facilities to better protect individually identifiable health information. Government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) stipulate how your digital records containing sensitive patient information should be kept secure, ensuring that your patient’s privacy is maintained. The consequences for violating Doctor / Patient confidentiality, even unintentionally, can be costly.

Yet, to date protecting your patients private data has been assiduous work requiring great attention to detail on a variety of fronts. Securely transmitting digital information via normal email opens you up to a host of patient privacy issues. Simply emailing a document to an intended recipient could potentially violate a patient’s privacy, since the email could be intercepted in transit or read by unintended persons on the destination email server before it is downloaded. Using normal email, it is nearly impossible to tell whether or not the document was tampered with or was sent by someone electronically pretending to be someone else. And legal experts agree, the “email disclaimers” often found at the bottom of emails cannot protect the privacy of information contained in an email, nor guarantee that you will be not be held liable for this misuse of that information. The “email disclaimer” provides no real prevention for security breach of your information.

Whether you are a healthcare provider, payer or pharmaceutical company, you have electronic information that must be protected. eCipher from Essential Security Software® virtually eliminates the costs associated with safeguarding the transit of Electronic Patient Health Information (PHI). With eCipher you can easily and securely email medical advice to your patients, send prescription requests to the smallest of pharmacies and safely deliver patient records to referral doctors.

## Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was designed to create a new national standard for protecting the privacy of patient's health information. HIPAA also focused on improving the efficiency and effectiveness of the Healthcare system, by encouraging the development and adoption of Electronic Data Interchange (EDI) between healthcare providers, payers and pharmaceutical organizations. HIPAA also stipulates the strict requirement for organizations to establish safeguards to protect the integrity and confidentiality of an individual's Protected Health Information (PHI).

HIPAA applies to individual healthcare providers, health plans, and healthcare insurance providers. The law also pertains to organizations that deal with the electronic PHI of customers, employers and patients. Civil and criminal penalties can result from noncompliance and security violations.

## Penalties for HIPAA Violations

HIPAA calls for civil and criminal penalties for security and privacy breaches. General failure to comply is \$100 per penalty; violations of an identical requirement may not exceed \$25,000 per year. For example: it would be considered a violation to email claim or file with identifiable patient information that is not encrypted. Even though one requirement may not exceed \$25,000, HIPAA has more than 15 named security standards, which if repeatedly violated could quickly grow to more than \$375,000.

More severe criminal penalties also apply to more flagrant HIPAA violations. Wrongful disclosure of PHI can result in a \$50,000 penalty and up to one year in prison. An offense with intent to sell or misuse patients protected health information is punishable with a maximum \$250,000 fine and/or 10 years imprisonment.

## Common HIPAA Scenario Crises and the eCipher Solution

Medical office wishes to refer an identifiable PHI to another healthcare provider. A primary care physician examines an individual and determines that he would like to send the patient to another provider for further diagnosis or treatment. The physician then asks his/her assistant to assemble and email the patient's history and physical (H&P), imaging reports, labs, progress notes, etc. to the off-site healthcare provider for review. Unfortunately, the physician and his assistant are now in violation of HIPAA regulations.

Unprotected email is like sending a postcard through cyber-space, making it easy prey for theft and tampering. While in transit, it is routed through multiple servers and consequently an email containing patient PHI can be easily read by people other than the designated recipient (the off-site provider). Furthermore, the patient's records, because of an accidental keystroke, could be unintentionally forwarded to an unknown party, thereby increasing the severity of the security breach.

The physician's assistant could have used eCipher to protect the email and attachments. The outgoing documents would be encrypted and un-accessible to anyone besides the intended recipient healthcare provider. Even if the receiving healthcare provider is not fully set-up to work with electronic patient healthcare information, they can still securely view patient records without violating patient confidentiality.

## On-line Pharmaceutical Providers

A pharmaceutical provider fills prescriptions via on-line ordering, but cannot meet HIPAA secure transmission requirements for emailing regarding prescriptions and medications, order confirmation, and other information to their patients. The organization could resort to analog methods such as calling each individual customer or sending information to the customers via standard post. However, these methods are very inefficient and cost prohibitive. To meet HIPAA regulations, the on-line prescription provider must shoulder the burden of hiring and training a number of new employees at great cost. What is the on-line pharmacy to do?

With eCipher, the pharmaceutical provider can securely send prescription information, order confirmations and more to their clientele. The confidentiality and integrity of email containing protected health information (PHI) is enforced and maintained even after delivery. With the eCipher "Anywhere" web-delivery feature, people can access their secure, confidential email on their computer or mobile device<sup>1</sup>.

eCipher's additional protections enable a company with an effective way to control how the email content can be used. These options can be set to prevent the forwarding, printing or copying of email content. "Delivery Receipts" notify a company of who opened a particular message and when it was read.

## Healthcare Providers to Communicate with Patients via Email

To provide added value, a healthcare provider wishes to establish an easy and affordable way to give their patients medical advice over the web. The provider must have the ability to send and receive protected medical advice from work or home but does not want to invest in the installation, maintenance and expensive licensing fees associated with available server-based solutions. Furthermore, the caregiver's patients are largely non-technical and will not bother with cumbersome key exchange, s/mime and other requirements commonly associated with widely available encryption

---

<sup>1</sup> iPhone, BlackBerry or Windows Mobile 6 or newer.

technologies. Additionally, encryption software does not prevent forwarding and copying of content after it has been delivered.

Once opened, a patient's identifiable medical information is totally exposed; email can be accidentally forwarded, laptops and PCs can be lost or sold with PHI remaining on the hard-drive, patient info could be leaked via virus, spy-ware or Trojan worm. Unintended individuals can gain access and doctor-patient confidentiality is breached. The caregiver must be able to ensure that email sent with sensitive information is protected from theft and misuse, during transit and even after it has arrived in a recipient's inbox. How can the healthcare provider utilize the power of email to give medical advice whilst keeping sensitive patient data secure?

eCipher helps healthcare professionals meet HIPAA requirements for the secure storage, transmission and delivery of electronic patient information. eCipher makes the sending and receiving of protected email and attachment quick and easy. From the desktop application or using the Microsoft Outlook® add-in, Healthcare Providers can encrypt and apply anti-theft controls to prevent forwarding, cut/copy/paste and printing.

## ECipher: Facilitating HIPAA Compliance

eCipher from Essential Security Software can help your organization comply with HIPAA electronic transmission regulations. eCipher is by no means a comprehensive overall HIPAA security solution, however if used properly can help your business to meet the following rules:

HIPAA Rule	Security Procedure	Description	The eCipher Solution
164.312(e)(1)	<b>Ensure Transmission Security. (Required)</b>	“Implement technical security policies and procedures measures to guard against unauthorized access to electronic protected health information (E PHI) that is being transmitted over an electronic communications network.”	eCipher ensures the security and integrity of email & files before, during and after transmission. Protected files are securely encrypted and can only be accessed by the intended recipients.
	<b>Implement Encryption</b>	“Encrypt E PHI whenever deemed appropriate.”	Easily encrypt emails containing E PHI. Every message sent with eCipher is strongly encrypted.
	<b>Implement Integrity Controls</b>	“Implement security measures to ensure that electronically transmitted E PHI is not improperly modified without detection until disposed of.”	Usage permission controls prevent alteration of E PHI. Files are persistently protected. eCipher prohibits forwarding, printing, cut/copy/paste, unauthorized access and more.
164.312(c)(1)	<b>Access Control. (Required)</b>	“Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.”	Secure email and files can only be opened by authorized individuals.
	<b>Implement a Mechanism to Authenticate E PHI</b>	“Consider possible electronic mechanisms for authentication such as: digital signatures, error correcting memory...”	Digital signatures and encryption ensure secure transit, storage, integrity and authentication.
164.310(d)(1)	<b>Device and Media Controls. (Required)</b>	“Implement policies and procedures to address the final disposition of E PHI, and/or the hardware or electronic media on which it is stored.”	Protected files can only be opened by authorized individuals.

## eCipher Features and Benefits

- Gives off-site providers an easy method to securely email PHI sent across disparate computing environments.
- Helps ensure authenticity of EPHI with digital signatures.
- Improve productivity by using the web to instantly & securely share sensitive data
- Prevents unauthorized forwarding, cut/copy & paste, or printing of an email.
- Ensures a sent email is legitimate and is not intercepted, tampered with or altered.
- Deliver secure messages to anyone with no download required.
- Easiest-to-use email encryption enables anyone to use eCipher.
- Meets regulatory compliance requirements for privacy - HIPAA, PIPEDA, NRS 597.970, 21CFR Part 11, Sarbanes-Oxley

## Decreasing Your Vulnerabilities

No security software in the world is 100% unbreakable. Even the most advanced digital cryptography techniques can be broken or circumvented by some person or organization with enough motivation, time and money. eCipher considerably reduces the risk that sensitive data can be accessed and stolen beyond the intended recipient. Applied safeguards remain with the data no matter where it travels or where it is stored. Even if a CD or USB thumb-drive containing protected data is stolen, the information contained therein will remain protected and cannot be opened by unassigned recipients.

## Summary

Unprotected electronic files containing sensitive data can easily be accessed, altered, stolen and re-distributed to unintended parties. Electronic protected health information (EPHI) is subject to stringent HIPAA regulations; penalties for violation of HIPAA rules can result in stiff fines and jail time. Loss of EPHI can place healthcare organizations at great financial and legal risk. eCipher, from Essential Security Software can help small to mid-size healthcare providers mitigate these risks, affordably and with no technical training or knowledge needed.

eCipher opens up a new realm of possibilities for healthcare organizations that have been unavailable until now. Healthcare providers can securely email medical information to their patients. Pharmacies can use eCipher to send prescription order information to doctors and customers alike. Healthcare providers can quickly and securely collaborate with off-site specialists thereby ensuring patients receive good treatment and much more.

## Evaluate eCipher for Free

Your company can evaluate eCipher for free to send and view protected email. To get a free evaluation copy, please visit <http://www.essentialsecurity.com/products.html> and click the “Download Now” button.

## Our Commitment: “The Customer Comes First”

Essential Security Software is committed to providing our customers with the highest level of support. As a eCipher customer, you can expect to be treated with the utmost professionalism, honesty and respect. We will put forth the extra effort to best answer all of your inquires in a knowledgeable, courteous, and speedy fashion.

Our support team is available to assist customers Monday through Friday from 9:00 AM through 5:00 PM PST, excluding holidays.

### **Support desk contact information:**

Email: [support@essentialsecurity.com](mailto:support@essentialsecurity.com) Tel: +1(888) 454-2632 or +1(425) 454-2632