

# Securing the Medical Office with Taceo

## OVERVIEW

Operating a medical practice is assiduous work requiring great attention to detail on a variety of fronts. Patient privacy has always been an important concept in the medical profession. New laws are taking this notion a step further, making it mandatory for medical facilities to protect individually identifiable health information. Government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and others stipulate the how your digital records containing sensitive patient information should be kept secure, but caring for your patient's privacy is just good business.

One of the most time and labor consuming tasks in maintaining an electronic medical record is importing non-digital patient information such as radiology reports, hospital dictation and consultation/referral letters is an extremely time and labor consuming task in maintaining an electronic medical record. This is unfortunate because most of this information is already in digital format at the sender's location but printed to paper for transit. Transmitting digital information securely, however, can be problematic at best. Simply emailing a document to an intended recipient would potentially violate a patient's privacy since the mail could be intercepted in transit or read by unauthorized persons on the destination email server before it is downloaded. Also, it would be impossible to tell whether or not the document was tampered with or was sent by someone electronically pretending to be someone else. For example, to promote office efficiency, medical offices that want to allow physicians to provide electronic mail as a means to transmit information are forced to have an "email disclaimer" that can not guarantee the privacy of information contained in an email. The information may be confidential and subject to protection under the law, but the fact remains that no real protection is provided as a preventative for security breach of your information.

Whether you are a healthcare provider, payer or pharmaceutical company you have electronic information that must be protected. Essential Taceo virtually eliminates the costs associated with safeguarding Protected Health Information (PHI). With Taceo you are now free to 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. Offense with intent to sell or misuse patients protected health information is punishable with a maximum \$250,000 fine and/or 10 years imprisonment.

## TACEO: HELPING TO NAVIGATE THE HIPAA MINEFIELD - COMMON HIPAA SCENARIOS AND TACEO

Medical office wishes to refer and 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 in now violation of HIPAA regulations.

Unprotected email is like sending a post-card through cyber-space. While transiting it is routed through multiple servers, 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 misdirected to an unknown party, thereby increasing the severity of the security breach. The physician's assistant could have used Taceo to protect the email and attachments. With the quick click of a button the worker could have prohibited the patient records from being printed, forwarded and edited. 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 Provider

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 Taceo, the pharmaceutical provider can securely send prescription information, order confirmations and more to their clientele. The confidentiality and integrity of emails containing protected health information (PHI) is enforced and maintained even after delivery. Nearly any customer with a PC1 can easily download the free version of Taceo, enabling them receive and reply protected email.

Taceo's usage permissions interface provides the company with an effective way to assign flexible rights management controls based on the profile of the client. Emails Containing prescription information can be set to expire when no longer valid.

Healthcare giver wishes to provide individual patients medical advice 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 and cannot afford 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 technologies.

Additionally, encryption software does not protect content after it has been delivered. Once opened, the 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. Unauthorized individuals gain access and doctor-patient confidentiality is breached. The caregiver must be able to ensure that received documents remain encrypted and can be deleted from the patient's computer after a given time. How can the healthcare provider utilize the power of email to give medical advice while keeping sensitive patient data secure?

Taceo helps healthcare professionals meet HIPAA requirements for the secure storage, transmission and delivery of identifiable patient information. Taceo makes the sending and receiving of secured email and documents quick and easy. From the desktop or MS Outlook®, providers can encrypt and apply usage permissions to control and prevent actions as forwarding, cut/copy/paste, printing and disabling the Print Screen key. Email and documents can also be set to "expire" and will become unreadable at a given time and date.

Taceo is by no means a comprehensive overall HIPAA security solution, however if used properly can help your business to inexpensively meet most of the critical rules.

#### TACEO FEATURES AND BENEFITS

- Protect EPHI from theft, misdirection and unauthorized distribution.
- Allows primary care providers and specialists to instantly and securely share patient records with little cost.
- Enables patients to easily access and securely reply to protected emails containing medical advice, prescription information and more from their home or work computers.
- Gives off-site providers an easy method to access and reply to secure email sent across disparate computing environments
- Affordable security beyond the office firewall. Taceo can ensure the proper use and protection of EPHI no matter where it travels or where it is stored.
- Helps ensure authenticity of EPHI with digital signatures.
- Improve productivity by using the web to instantly & securely share sensitive data.
- Taceo offers an affordable way to securely store sensitive information on site.
- Prevent unauthorized access to your documents.
- Prevent unauthorized distribution (no forwarding)
- Prevent document editing (no cut, copy, paste)
- Set expiration time/date on email & documents.
- Ensures confidentiality and privacy.
- Securely and permanently delete files to Department of Defense standards (DOD 5220.22-M).
- Patients can download Taceo for free.
- Meet regulatory compliance requirements for privacy - HIPAA, PIPEDA, 21 CFR Part 11, Sarbanes-Oxley

## REDUCING YOUR VULNERABILITIES

No security software in the world is 100% unbreakable, even the most advanced digital encryption techniques can be broken or circumvented by some person or organization with enough motivation, time and money. Taceo does not totally negate the risk of information leakage, for example a malicious individual could take a digital photo of the screen or re-type the content into another document and distribute it. However, Taceo considerably reduces the risk that sensitive data can be disseminated to unauthorized individuals or groups. Taceo 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 encrypted and cannot be opened by unauthorized recipients.

## THE ANALOGUE TO DIGITAL MIGRATION

Although it is often difficult to make the initial switch to using digital patient records, the cost savings can be profound, especially when amortized over a number of years. Benefits include better accuracy in health records, less time spent transcribing patient notes, filling prescriptions and receiving quicker payment from insurance companies. For the most part many healthcare practitioners have been slow to adopt digital medical records, as of April 2005 only 16.4% of doctors in the United States had made the switch. Reasons most often cited for the slow adoption has been the costs in time and money. Fear of complicated regulations also slow the transition; once records are in the digital realm HIPAA standards must be strictly adhered.

Although the task appears daunting, individual and smaller medical practices can cost-effectively make the digital transition with largely low cost, off-the-shelf components.

Taceo, from Essential Security Software should be an integral part of any digital migration plan. Taceo can help your office secure the storage and transmission of PHI. Because Taceo can be used on almost any PC, it can be used to "bridge the gap" with offices of other healthcare providers that have not yet made the switch to digital records. Whether digital or analog, all organizations that deal with patient medical information are subject to HIPAA ordinances.

## SUMMARY

Any healthcare provider or organization that works with patient healthcare data is at risk for losing control of this information. Unprotected electronic files containing sensitive data can easily be accessed, altered, stolen and re-distributed to unauthorized 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.

Taceo, from Essential Security Software can help small to mid-size healthcare providers mitigate these risks. Taceo can also help organizations meet HIPAA requirements for the secure transmission, access and integrity of EPHI. Taceo is effective, affordable and easy-to-use software that enables healthcare providers to securely store, transmit and receive sensitive data. Taceo can encrypt and help control access to almost any file. Protected email and documents are safeguarded against unauthorized forwarding, editing, copying, and printing or screen capture. Taceo opens up a new realm of possibilities never available before with such ease and affordability. Healthcare providers can securely email medical information to their patients. Pharmacies can use Taceo to send prescription order information to doctors and customers alike.

Caregivers can quickly and securely collaborate with off-site specialists thereby ensuring patients receive good treatment and much more.

System Requirements • Microsoft Windows 2000/XP/2003 or newer • Microsoft .Net framework installed (if you don't have this Taceo will install it for you) • Internet access. • 15 MB of available hard-drive space

Visit [www.essentialsecurity.com](http://www.essentialsecurity.com)

## About the Author

Providence Health System is a major health care provider and insurer in four. We wanted a Web site that could become a core system.

Source: <http://www.productsherbal.com>