Security and the Digital Healthcare Transformation

Healthcare Drives Improvements to Secure Information

CipherPost Pro:

- Secure Messaging
- Secure File Sharing
- Message Control
- Secure E-Signatures

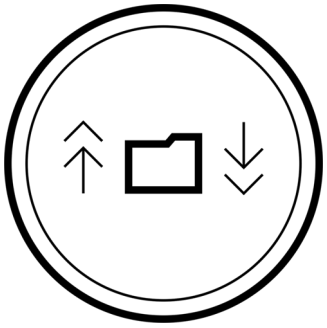
Optimized for Office 365

Introduction

When it comes to efficiency, healthcare organizations face unique challenges. The urgent nature of healthcare makes both expedience and accuracy absolutely crucial. Information travels through numerous touchpoints, including doctors, nurses, patients, insurance providers and laboratories, and priorities shift rapidly as crises or emergencies occur at a moment's notice. Meanwhile, all of this data must be exchanged rapidly, yet securely, ensuring that patient confidentiality and data privacy are protected along every step of the workflow. This push for efficiency and cost savings has driven healthcare organizations to move from paper files and fax communications to cloud-based, secure digital information workflows.

Opportunities for Improved Efficiency

Moving from paper forms, fax, courier and mail to digital files and secure communications saves time and money for healthcare professionals in a variety of roles. X-rays can be emailed from technicians to doctors; charts and lab results can be shared among doctors and specialists; insurance claims can be expedited; and medical forms can be filled out and signed electronically. When these transactions are authorized and secured throughout the exchange, healthcare workers increase productivity and patients provide and receive information faster, without worrying that their medical information is at risk.



Typical Healthcare Information Workflows

Provider to Provider

- Transfer patient medical histories/charts
- Deliver lab results
- Share x-rays and other scanned images and results
- Transmit provider agreements to be signed

Provider to Patient

- Request consultations
- Make appointments
- Provide notice of privacy practices
- Send new patient forms and consents to be completed before an appointment
- Provide HIPAA and other regulatory forms and notifications

Provider to Payer

- Process and expedite claims
- Deliver lab results
- Bill and invoice insurance forms, reducing the cost of paper billing
- Request and expedite authorizations for treatment

Internal to Provider

- Update medical records
- Sign x-rays and other medical record reviews

Often, healthcare organizations view the move to electronic data as a tradeoff between efficiency and privacy.

Issues and Concerns with Electronic Health Information

Often, healthcare organizations view the move to electronic data as a tradeoff between efficiency and privacy. How useful are cost savings and increased productivity if patient data confidentiality is compromised? And conversely, how beneficial is air-tight security if it impedes a provider's ability to onboard and treat patients quickly and effectively?

To address these concerns, the latest information technologies need to address the following issues:

- Availability
  Enable authorized users to access and use paper and electronic health information on demand.
- Privacy
  Ensure that all health data remains protected and accessible by authorized workers only.
- Integrity
  Guarantee that no information is approved, altered or destroyed without proper authorization.

194 Breaches at Healthcare Providers Were Reported in 2015.

U.S. Department of Health & Human Services Office for Civil Rights Breach Portal

26% of Breaches Were Caused by Individuals Emailing Data to Incorrect Individuals.

Verizon 2016 Data Breach Investigations Report

Threats to Healthcare Data Sharing

Data breaches occur for a variety of reasons, including from hackers, unintentional email mistakes, intentional data leakage, theft or misplacement of laptops and electronic devices, and unauthorized access to servers and files. The consequences of unauthorized disclosure of private patient healthcare and financial information are significant and include hefty fines and penalties for noncompliance, lawsuits, and damaged reputations. For example, since 2009, the protected health data of approximately 31.4 million people in the U.S. has been compromised in security breaches, resulting in $25.1 million in fines against healthcare organizations, according to Gartner.

A separate report by the BBC reported that, in England, the National Health Service (NHS) experienced several breaches over a three-year period between April 2011 and April 2014. Big Brother Watch found 7,255 recorded incidents during that same time, with some data being posted on social media, or lost, or stolen. In many cases, data was shared with a third party inappropriately, and in 236 instances, data was shared by email, letter, or fax.

Some of the largest breaches have occurred not with electronic files but with paper. For example, the Indiana Parkview Health System was fined $800,000 after it was determined that 71 boxes of patient files were left in a doctor's driveway while she was away.

Cases such as this disabuse the notion that paper, fax, or mail is more secure than digital files, and in instances where email was misused, the breach likely would have been prevented with the right email security and controls in place.

More Devices, More Concerns: BYOD

Increasingly, doctors, nurses, and other healthcare providers are using portable devices such as smartphones and tablets on a regular basis as they move from location to location, do their rotations, etc. As such, healthcare organizations require a way to secure communications from personally-owned devices, ensuring that data isn't intercepted or sent incorrectly from devices the organization cannot control. This is where cloud-based solutions, such as secure email, are especially useful, enabling users to exchange information securely, regardless of device or location.

More than half of U.S. hospitals use smartphones and/or tablets and 69% of clinicians use both a desktop/laptop and a smartphone/tablet to access information.

The 2014 HIMSS Analytics Mobile Devices Study

Regulatory Compliance

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the U.S. healthcare industry to protect individuals' health information while facilitating the exchange of information needed to provide quality care. Two HIPAA provisions apply specifically to email policy and security: the Privacy Rule and the Security Rule. Together they identify what information should be protected and provide a security framework for organizations to ensure email compliance.

With so much medical and financial information circulating, organizations need to consider secure messaging and file-sharing solutions that conform to HIPAA requirements without compromising the functionality and workflow of their existing email.

Complying with organizational policies as well as HIPAA requires healthcare organizations to look for email security solutions that add full security without adding excessive costs and complexity. In the past, this has been a balancing act, but with the latest cloud-based technologies, protecting and enabling rapid exchange of information among authorized healthcare users has become easier.

From Issues to Opportunities

In addition to making data exchange safer and easier, cloud-based email is embraced more and more as a business tool for healthcare organizations. Now physicians consult with each other and patients without leaving the office. Healthcare providers bill patients quickly, and patients submit health insurance claims online. Laboratory results and scans are commonly shared over desktop or smartphone to help speed diagnoses.

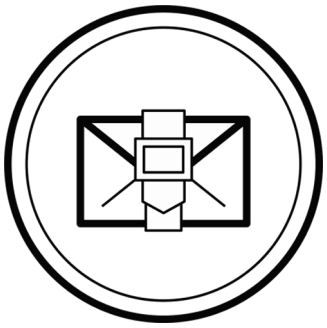
With so much medical and financial information circulating, organizations need to consider secure messaging and file-sharing solutions that conform to HIPAA requirements without compromising the functionality and workflow of their existing email. In short, messaging security should complement existing email, not complicate it. This means implementing a solution that allows easy and scalable deployment, simplifies management complexity, and works with your existing email infrastructure to enable user productivity and email functionality. Organizations should ask specific questions about any new solution, including:

1. Does the solution integrate seamlessly into existing infrastructure? Does it require additional hardware or IT expertise or does it deploy easily and quickly?

2. Does the solution enable authorized clinicians to securely sign documents electronically from within their email clients? Are the communications tracked and secured throughout the process to meet HIPAA requirements?

3. Will users be able to securely share large files such as x-rays without requiring additional applications?

4. Does the same high level of security and convenience extend to mobile devices?



CipherPost Pro Makes It Secure and Simple to Share, Approve, and Comply

AppRiver helps organizations capitalize on healthcare's digital transformation by solving the concerns discussed previously and delivering a workflow tool that offers more than just encryption. AppRiver CipherPost Pro enables healthcare professionals in any authorized role to share, track, and control health-related records and files securely. Moreover, CipherPost Pro becomes a productive tool, enabling clinicians to e-sign and authorize workflows and exchange large files without jeopardizing data integrity or privacy.

AppRiver CipherPost Pro integrates easily into common email programs and is fully functional on mobile devices, providing your users with secure messaging, e-signatures, file sharing, and message tracking right in their existing email using existing email addresses.

CipherPost Pro helps healthcare organizations achieve efficiency and security by allowing physicians, nurses, medical records assistants, insurance providers, patients, and others to:

- Share files, medical records, and patient data while complying with regulations
- Encrypt data in one click for full protection, from sending through to archiving of messages
- Share large files securely, including medical scans
- Fully track, control, and recall messages and documents
- E-sign documents, records, and more, legally, without leaving the email client
- Capture information (consultations, insurance claims, etc.) from websites through Secure Web Forms

AppRiver CipherPost Pro integrates easily into common email programs and is fully functional on mobile devices, providing your users with secure messaging, e-signatures, file sharing, and message tracking right in their existing email using existing email addresses. There is minimal disruption to users and getting up and running takes just minutes.

Office 365

Optimized for Microsoft Office 365, AppRiver CipherPost Pro makes it easier for healthcare organizations to improve efficiency through sharing secure messages and files and authorizing e-signatures on documents. CipherPost Pro increases patient satisfaction while protecting private patient data and ensuring compliance.

About AppRiver: Cloud-based Cybersecurity Solutions for Business

AppRiver is a Software-as-a-Service (SaaS) application provider offering award-winning email and Web security solutions to businesses of all sizes. Understanding the need to protect networks from today's increasingly complex IT threats, AppRiver offers businesses a comprehensive, yet affordable subscription-based solution that incorporates the latest spam and virus protection, email encryption and Web security on the market. In addition, the company provides a complete managed service for Microsoft Exchange, as well as a bundled Office 365 solution.

Call 1.866.223.4645 for more information about AppRiver and to get a

CIPHERPOST PRO FREE TRIAL