WHAT YOU NEED TO KNOW ABOUT HIPAA COMPLIANCE AND CLOUD SERVICES

A Guide for Healthcare Providers and Their Business Associates

As a health care provider or business associate, you’re at the center of a confluence of forceful trends:

- With the Affordable Care Act, more and more patients have access to healthcare.
- HIPAA and other laws and regulations demand rigorous protection of sensitive patient data and protected health information, and impose severe penalties for those business associates that fail to comply with such requirements.
- As always, you need to maximize cost efficiency—which means, among other things, spending wisely on information technology (IT) that’s integral to modern health care delivery and management.

This guide for health care administrators and IT managers summarizes what you need to know—and do—to help ensure that your email, voice communications, and other cloud-based information management tools and processes are in full compliance with HIPAA’s requirements. And it describes how you can do so easily and cost-effectively.
Email: Central to Your Services—and Your Risks

Now central to our lives in so many ways, email communication is integral to everything you do as a healthcare provider. It not only connects your staff with its patients (and each other), but with its many partners as well: insurers, pharmacies, specialists, service providers, and others.

Think how many emails you generate every day: appointments, referrals, insurance claims, authorizations, lab results, answers to patients’ questions, and more. How many contain protected health information that requires protection under HIPAA? And how many of those sensitive emails pass beyond your own presumably secure network—to and from possibly insecure third parties, including your employees’ and partners’ mobile devices? If you do not have a secure network provider, every such email is a possible point of regulatory vulnerability or violation.

Based on your status as a covered entity under HIPAA, your staff members are authorized to send and receive, among themselves, Protected Health Information (PHI) (or ePHI, when in electronic form). But your responsibility for protecting the privacy and security of such information for your patients doesn’t stop there. Just like your email, it often goes beyond the security of your network.

HIPAA and HITECH: Rights for Patients, Rules for Providers

Passed by Congress in 1996, the Health Insurance Portability and Accountability Act mandates a set of regulations protecting the privacy and security of patients’ confidential health information, including when and with whom that information can be shared.

A supplemental Privacy Rule regulates the use and disclosure of patient data—whether verbal, written, or electronic—for health care providers, health plans, and health care clearing houses, all known as covered entities. A Security Rule specifically defines security standards for the management of health information in electronic form (ePHI) by covered entities.

The Health Information Technology for Economic and Clinical Health (HITECH) Act (2010) and the HIPAA Omnibus Rule (2013) strengthens HIPAA’s privacy and security rules and toughens the penalties for breaches in patient privacy and health information security.

It’s important to note that covered entities must be in compliance with HIPAA’s privacy standards even if they contract with vendors to perform some of their essential functions. In other words, your responsibilities and liabilities under HIPAA extend to all of your business associates. These include labs, billing offices, clinical services, and the like, as well as the providers of your cloud-based IT services.
Is Your Email System Compliant?

Don’t assume that all business email systems are compliant with HIPAA. Many systems, including several well-known brands designed for professional or even enterprise-level use, are not.

Chances are, your internal email is safe on your own secure servers and your email to and from third parties, including all email that contains PHI, is probably encrypted, as required by HIPAA. But encryption is not enough.

HIPAA requires that the technical safeguards for your email system and practices fall into three main categories:

**Access control and authentication.** A covered entity must implement policies and procedures that only allow authorized personnel to access ePHI. For example, each of your staff members must have a unique username and password for identification and tracking purposes. Shared logins are not permitted. Furthermore, you must have procedures for verifying that anyone seeking access to ePHI is who they claim to be.

**ePHI security and integrity, in storage and during transmission.** You have to protect ePHI from being improperly altered or destroyed. Beyond storing ePHI securely, this means you must also have technical security measures, including encryption, in place to prevent unauthorized access by anyone who might tamper with ePHI while it’s being transmitted out of your network.

**Audit controls.** You have to have the hardware, software, and processes in place to record and monitor all logins to your health care information systems (including date, time, and IP address) and track all sent and received emails.

Remember, the same requirements apply to covered entities with whom you communicate and share protected information with via email. In fact, they apply to any and all persons and organizations—including cloud IT providers—that you outsource your essential business services to.

Protecting Patient Records with Secure File Sharing and Syncing

Your handling and use of confidential patient health information includes more than just email content and attachments.

Digital health records are essential to health care and administration. Multiple parties, both inside and outside of your organization, need access to your patients’ electronic health information and that imposes a complex set of requirements on your IT systems, including:

**Security.** Again, HIPAA imposes an absolute responsibility for safeguarding patients’ health records, both at rest and in transit. This means you have to control multiple levels of access to that information for the many people who collaborate on patient care and related services—this includes your many diverse partners as well as your staff. You also have to be able to monitor and audit any person, both inside and outside of your organization, who has access to or use of such records.

**Integrity.** To secure ePHI from improper change or destruction, you must control not only who has access to what information but also who can change a file and when.
**Mobility.** Mobility has come to medicine. You may already be deploying authorized mobile devices, such as wifi-connected cart-based PCs in hospital wards or personal tablets for clinicians. Nowadays, more employees use their mobile devices to connect to network-based applications and files. Some employees will use mobile devices issued by you while others will use their own personal mobile devices (a trend known as BYOD, or bring-your-own-device). Mobility adds another significant layer of complexity to the task of safeguarding their patients’ PHI.

**Beyond Email and Documents: HIPAA-Compliant Voice Services**

The requirements of HIPAA for voice communications are not, perhaps, as obvious as they are for email and document security. But yes, HIPAA does require you to safeguard PHI for voicemails and call recordings that are recorded as computers files.

Like email, voice communications are myriad. They occur not only between your clinicians, patients and among your staff, but also between your organization and many parties outside of your organization, such as specialists, pharmacies, and the many other service providers and business partners with whom you need to share patient information.

As with email and documents, HIPAA requires you to maintain the privacy of your patients’ voicemail content and voice accounts through strictly controlled access, secure transmission and storage.

**Command and Control:**
**Your Responsibility—and Your Best Protection**

It’s not as if you wouldn’t want total security and control for the storage of your email, health records, voicemails, and other systems in any case. It’s just that, under HIPAA, it’s the law—and a very exacting law at that.

Under HIPAA, you must be able to track and report all emails sent inside and outside of your network. But you also have to be able to track and verify access to ePHI at every attempt. In fact, you must have systems and procedures in place to record and analyze all activity in your systems that store or use ePHI. And you must be able to document the access and security controls you have in place to protect patient privacy in your voice communications as well.

Such audit and reporting capabilities are not just your responsibility. They are also your best protection. They enable you to maintain your systems’ performance and compliance at peak levels and spot vulnerabilities before they escalate into problems. And they give you the data you need to demonstrate your compliance. That’s essential, because HIPAA requires not just that you comply with its broad set of requirements, but also that you be able to prove your compliance through regular audits and in the event of an inquiry or claim.

**Easy, Reliable, Economical:**
**Empiretech Hosted Services for Health Care Entities**

Empiretech Office in the Cloud™ delivers an integrated set of hosted email, file sharing and syncing, hosted PBX and voicemail, and other essential services for health care providers and

Empiretech

518-557-1122 empireinfo@empiretech.net www.empiretech.net
other covered entities. These services are protected by robust security, access control, and identity management technologies and can be easily managed via Empiretech’s central control panel. Empiretech provides a comprehensive Business Associate Agreement (BAA) that acknowledges our role and responsibilities under the 2013 HIPAA Omnibus Final Rule. This legal document stipulates that we will safeguard all patient health information stored on Intermedia systems. It certifies that our systems have been audited to assess compliance with HIPAA’s data privacy and security requirements by an independent third party. And our BAA details how Empiretech will support you in the event of an audit, inquiry, or claim regarding your own compliance.

Together, Empiretech solutions for health care entities can help ensure your compliance with HIPAA’s mandated privacy and security regulations while streamlining your operations and reducing IT capital and operating expenses. For you, there’s no hardware to buy and no software to manage.

Empiretech technology, services, policies, and procedures have been evaluated by accounting and consulting firms for conformance with HIPAA data privacy and security requirements.
# What HIPAA Requires, Empiretech Delivers

<table>
<thead>
<tr>
<th>HIPAA requires …</th>
<th>Empiretech Office in the Cloud provides …</th>
</tr>
</thead>
</table>
| **Access control and authentication:** | Email services:  
- Unique IDs for users  
- Ability to identify and track all user actions  
- Procedures for verifying that anyone seeking access to ePHI is who he or she claims to be  
- Procedures for verifying that anyone seeking access to ePHI is who he or she claims to be  
- Procedures for verifying that anyone seeking access to ePHI is who he or she claims to be  
- Procedures for verifying that anyone seeking access to ePHI is who he or she claims to be |
| - Unique IDs for all users accessing ePHI  
- Ability to identify and track all user actions  
- Procedures for verifying that anyone seeking access to ePHI is who he or she claims to be  
- Procedures for verifying that anyone seeking access to ePHI is who he or she claims to be | Email services:  
- Unique IDs for users  
- Logging of user login/logout and admin account activity  
- Strong password enforcement capabilities at the administrative level.  
Voice services:  
- Secure cloud storage of voicemail content.  
- Strong access control of voice accounts, including voicemail  
- Centralized administration and security |
| **ePHI security and integrity:** | Email services:  
- Integrated anti-virus and anti-spam  
- Automated scanning of all outgoing email with rules-based detection and encryption of sensitive data including patient identification, Social Security numbers, and medical procedures  
- Standards-based PKI encryption technology  
- Integrated email archiving  
File sync and share services:  
- 256-bit encryption for at-rest and in-transit data  
- Unique encryption key for each account (much better than sharing keys between customers)  
- Secure file links sent inside and outside your organization  
- Centralized and user-controlled permissions  
- Locking features to prevent overwrites, conflicts, or deletions  
- Administrators can remotely wipe data from any device  
Global Intrusion Prevention System protects all Intermedia cloud services.  
Data center-level backup and file replication protects against loss or corruption of information.  
Secure datacenters guarded by video monitoring, motion detection, and access control technology as well as 24/7 security personnel. |
| - Security systems that guard against unauthorized access to ePHI during electronic transmission, whether in email and attachments or during the file-sharing process  
- Both electronic and physical security to protect ePHI wherever it is stored  
- Technology and policies to secure ePHI from improper alteration or destruction | Email services:  
- Integrated anti-virus and anti-spam  
- Automated scanning of all outgoing email with rules-based detection and encryption of sensitive data including patient identification, Social Security numbers, and medical procedures  
- Standards-based PKI encryption technology  
- Integrated email archiving  
File sync and share services:  
- 256-bit encryption for at-rest and in-transit data  
- Unique encryption key for each account (much better than sharing keys between customers)  
- Secure file links sent inside and outside your organization  
- Centralized and user-controlled permissions  
- Locking features to prevent overwrites, conflicts, or deletions  
- Administrators can remotely wipe data from any device  
Global Intrusion Prevention System protects all Intermedia cloud services.  
Data center-level backup and file replication protects against loss or corruption of information.  
Secure datacenters guarded by video monitoring, motion detection, and access control technology as well as 24/7 security personnel. |
<table>
<thead>
<tr>
<th>Audit controls and capabilities</th>
<th>Email services:</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Systems and procedures for recording and examining activity in IT systems that store or use ePHI</td>
<td>● Detailed tracking and reporting of all outbound emails</td>
</tr>
<tr>
<td></td>
<td>● 100% capture across platforms and devices, including mobile</td>
</tr>
<tr>
<td></td>
<td>● Unlimited storage for archiving emails</td>
</tr>
<tr>
<td></td>
<td>● Centralized control and simple, flexible searching, filtering, tagging, and recovery methods for email archives</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof of compliance</th>
<th>Comprehensive Business Associate Agreement (BAA) signed by Empire tech, stating that we will safeguard all patient health information stored in Intermedia systems.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● Covers all provided Office in the Cloud services</td>
</tr>
<tr>
<td></td>
<td>● Includes independent third-party auditing of Empire tech systems and services</td>
</tr>
<tr>
<td></td>
<td>● Empire tech will provide customer support in the event of an audit, inquiry, or claim</td>
</tr>
</tbody>
</table>

**Empire tech Health Care Solutions Highlights**

<table>
<thead>
<tr>
<th>Security, Access Control, &amp; Identity Management</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and security controls to safeguard electronic protected health information in compliance with HIPAA regulations across your IT deployments, including covered entities and business associates.</td>
<td>● Independent third-party auditing with an evaluation (HIPAA’s Acceptable Use Policy, or AUP) for conformance with HIPAA’s data privacy and security requirements</td>
</tr>
<tr>
<td></td>
<td>● Business Associate Agreements (BAAs) available for Covered Entities and Business Associates as required by HIPAA</td>
</tr>
<tr>
<td></td>
<td>● Annual Service Organization Control (SOC) audits</td>
</tr>
<tr>
<td></td>
<td>● Single sign-on authentication that combines security and efficient user access to email, file sharing, and other applications</td>
</tr>
<tr>
<td></td>
<td>● Centralized granular configurability enables selective, multi-level access by entity, department and job title, and other criteria</td>
</tr>
<tr>
<td></td>
<td>● Global Intrusion Prevention Systems (IPS) protects all services</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Email
Cloud-based Microsoft® Exchange email from the world’s largest independent provider of Hosted Exchange.

- 99.999% uptime
- More control and security than on-premises systems with less complexity
- Integrated shared calendars and contacts
- Flexibility: mix and match add-ons and services
- Mobile security tools (like remote wipe) and policy enforcement
- Integrated virus and spam protection
- Rules-based encryption provides easy custom content filtering and scanning of all outbound email.
- Encrypt outgoing emails with ease
- Tamper-proof archiving keeps your email securely archived, speeds eDiscovery, and eases the protection of intellectual property

File Backup & Share
Empiretech’s sharesync® business-grade data backup and sharing features help your staff and partners work more collaboratively—from anywhere, on any device.

- Automatic backup and syncing of files and folders across virtually all users and devices, desktop or mobile, and on any OS or web browser
- Send secure, password-protected links to your files both inside and outside your organization
- Protect files with at-rest and in-transit encryption
- User-set permissions to control access privileges
- Remotely wipe files from mobile devices when employees leave
- Simple, intuitive collaboration for all users, internal and external to your organization

Voice Services

- Hosted PBX with centralized access control of voice accounts and services, including voicemail
- Secure cloud storage of voicemail content

Empiretech: Your Single, Central Point of Control

With Empiretech, while your data and services are securely off your premises; your control is not. Your Empiretech control panel centralizes management of your services for simplified yet versatile policy-based administration from any browser.

Empiretech functions and conveniences include:

- Add, delete, and modify users and privileges for all applications and services.
- Monitor and manage permissions.
- Set up multiple levels of administrators.
- Integrate mobile device management quickly and easily.
- Remotely data-wipe or deactivation of lost, stolen, or compromised mobile devices.
- Delegate setup and management to non-specialized staff and enable user self-management with the My Services control panel.
- Provision new apps and services on the fly.