HIPAA and Cloud IT:
What you need to know

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 care.

- HIPAA and supplementary laws and regulations demand rigorous protections of patient privacy and health care information security—and threaten severe penalties for those who fall short.

- You need, as always, to maximize cost efficiency—which means, among other things, spending wisely on the 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 and other cloud IT services are in full compliance with HIPAA. And it describes how you can do so easily and cost-effectively.

It all starts with email

Email communication is integral to everything you do as a healthcare provider. It connects your staff not just with patients and with each other, but with your many partners as well: insurers, pharmacies, specialists, service providers, and others.

Think how many emails you generate every day: appointments and referrals, insurance claims and authorizations, lab results and answers to patients' questions, and more. How many contain HIPAA-protected patient health information? 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? 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, amongst themselves, Protected Health Information, or PHI (or ePHI, when in electronic form). But your responsibility for protecting the confidentiality of such information and the privacy of 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 are bound by HIPAA's privacy standards even if they contract with others to perform some of their essential functions. In other words, your responsibilities and liabilities under HIPAA extend to all your business associates. This includes labs, billing offices, clinical services, and the like. It also includes the providers of your cloud- based IT services.

Is your email system compliant?

Don't assume that all business email systems are compliant. 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 qualifies under HIPAA as containing PHI, is probably encrypted, as required by the law. But encryption is not enough.

The HIPAA requirements for your email system and practices fall into three main categories:

Access control and authentication. 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, undetected, 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.

And remember, the same requirements apply to covered entities with whom you communicate and share protected information via email. In fact, they apply to any and all persons and organizations to whom you outsource any function essential to your business - especially cloud IT providers.

Beyond email: File sharing and syncing

Of course, your handling and use of confidential patient health information is not just a matter of email content and attachments.

Ours is an age of digital health records and specialized, collaborative health care and administration. To deliver the best care efficiently and economically, multiple parties, both within and outside your organization, need access to your patients' electronic health information. But that imposes a complex set of requirements on your IT systems, including:

Security. Again, HIPAA imposes an absolute responsibility for maintaining the privacy and confidentiality of patients' health records, both at rest and in transit. This means you have to provide and control multiple levels of access to that information for the many people who collaborate on patient care and related services—that is, your many diverse partners as well as your staff. And you have to be able to monitor and audit all health information file access, use, and change both inside and outside your organization.

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 deploy authorized mobile devices, such as wifi-connected cart-based PCs in hospital wards and personal tablets for clinicians. Chances are, more and more employees want and need to connect with your network-based applications and files from mobile devices, whether issued by you or purchased by them (a trend known as BYOD, or bring-your-own-device). Mobility adds another significant layer of complexity to the task of providing secure, HIPAA-compliant file access (as well as email).

Command and control: Your responsibility—and your best protection

It's not as if you wouldn't want total command and control of your email, patient information, and other systems in any case. It's just that, under HIPAA, it's the law— and a very exacting law at that.

Again, it goes beyond email. Under HIPAA regulations, you must be able to track and report on all emails sent outside your network. But you also have 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.

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 blossom into problems. And they give you the data you need to demonstrate your compliance in the event of an external audit or inquiry.

Easy, reliable, economical: Hosted services for health care entities

Cloud Services delivers an integrated set of hosted email, file sharing and syncing, and other essential services for health care providers and other covered entities. All are protected by robust security, access control, and identity management technologies. And all can be easily managed via Control Panel, the central control panel. For you, there's no hardware to buy, no software to manage.

Together, our solutions for health care entities can help ensure your compliance with HIPAA-mandated privacy and security regulations while streamlining your operations and reducing IT capital and operating expenses.

One of the world's leading accounting and consulting firms for conformance has evaluated our technology, services, policies, and procedures with HIPAA data privacy and security requirements.

Our Advantage

Enterprise-grade security. Not all clouds are created equal. Ours is purpose-built to keep your data secure and protected with redundant carrier-grade firewalls, intrusion prevention systems and a dedicated team of security professionals relentlessly dedicated to the protection of your data. Video monitoring and access control technology as well as security personnel stationed round the clock at each site guard our ten world-class datacenters.

99.999% uptime—guaranteed. We give you a financially backed Service Level Agreement promising to keep your users connected and productive 99.999% of the time. That means you can expect less than 6 minutes of downtime over the course of a year. And if we fail to deliver, we'll compensate you for it.

Integrated to work together, customizable to work for you. We set up and provision your cloud to match your requirements, not ours. And all of our services are thoroughly integrated, enabling your users to focus on your work, not ours. The same goes for managing your Cloud Services: you have just one login, one password, one bill, and one source of support.

We're there for you, everywhere and always. Got an issue? Call our support staff any time, day, or night. Your call will be answered by a full-time employee. We answer our phones in under a minute. For your users, the transition from local to hosted services is seamless. And we'll continue to offer you features and strategic advice for gaining more and more value from your cloud.

Audited for HIPAA compliance and excellence. One of the world's leading accounting and consulting firms for conformance has evaluated our Cloud Services with HIPAA data privacy and security requirements.

Annual SOC 2 Type II reports. Our systems and controls for ensuring security, availability, and confidentiality of your data are audited annually in accordance with the standards of the American Institute of Certified Public Accountants.

Already using Microsoft Exchange? You're ahead of the game. If you already have Microsoft Exchange or Lync Software Assurance licenses in place, you can economize by reusing them to take advantage of our hosted services.

Highlights of our health care solutions

Security, access control, & identity management

Capital Business Systems offers 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.

- Independent third-party auditing with an evaluation (HIPAA Acceptable Use Policy, or AUP) for conformance with HIPAA data privacy and security requirements
- BAA addendums available for Covered Entities and Business Associates as required by HIPAA
- Annual SOC (Service Organization Control) 2 Type II audits
- Single sign-on authentication combines security and efficient user access to email, file sharing, and other applications.
- Centralized granular configurability enables selective, multi-level access by entity, department, and job title, and other criteria.
- Global Intrusion Prevention Systems (IPS) protects all services.

Email

Capital Business System's cloud offers:

- 99.999% uptime guarantee.
- 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 powered by McAfee.

Policy-based Encryption

- Rules-based encryption provides easy custom content filtering and scanning of all outbound email.
- Encrypt outgoing emails with ease.

Archiving

Capital Business System's email archiving keeps your email securely archived.

- Helps ensure HIPAA compliance.
- Speeds eDiscovery and eases the protection of intellectual property.

File Sync & Share

Capital Business System's ShareSync service helps your staff and partners work more collaboratively—from anywhere, on any device.

- Automatic syncing of files and folders across all users and devices, desktop and mobile, 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.

See how we meet specific HIPAA requirements

HIPAA requires:	We provide:
Access control and authentication: • 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.	Email services: • Unique IDs for users. • Logging of user login/logout and admin account activity. • Strong password enforcement capabilities at the administrative level. All services: • Centralized control over user access, authentication, and encryption policies.
Audit controls & capabilities • Systems and procedures for recording and examining activity in IT systems that store or use ePHI.	Email archiving services: • Detailed tracking and reporting of all outbound emails. • 100% capture across platforms and devices, including mobile. • Unlimited storage for archiving emails. • Centralized control and simple, flexible searching, filtering, tagging, and recovery methods for email archives. File sync and share services: • Audit log of all events on the service. • Admin file management.

ePHI security and integrity

- 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.

Contact Us

Capital Business Systems
sales@capitalmds.com
Ph: 970-266-5106
Fax: 970-266-5107

www.capitalmds.com