TATA COMMUNICATIONS

「HOW HIPAA IS CHANGING THE WAY YOU DO BUSINESS」

The essentials you need to evolve in the healthcare industry

CONTENTS

1.0 INTRODUCTION

The compliance landscape in healthcare

Cloud computing presents a new model for improving healthcare delivery and increasing the business flexibility of healthcare organisations — enabling greater operational efficiency, cost-effectiveness, and agility. These benefits have propelled the global market for healthcare cloud computing to grow at a CAGR of 11.6% during 2017-2022, on track to reach USD $35 billion by 2022.[1]

However, healthcare is a highly regulated environment, and the nature of cloud computing infrastructure escalates concerns over privacy, security, access and compliance. In fact, data breaches impacted the Protected Health Information (PHI) of nearly 15 million people in 2017, most incidents being hacking or IT related.[2] So, while the benefits are apparent, moving PHI beyond the secure perimeter of the healthcare organisation and accessing it via a diverse range of devices and locations is concerning.

To protect PHI, the USA enacted the Health Insurance Portability Accountability Act of 1996 (HIPAA). The privacy standards were designed to protect patients' medical records and specified health information. The Act was amended in 2009 and 2013 to further strengthen the privacy and security norms.

HIPAA has since established appropriate safeguards to protect PHI residing not only with healthcare providers but also their business associates, such as third party vendors or contractors such as Cloud Service Providers (CSP).

This makes it important for healthcare providers to ensure their business associates have a highly secure and auditable infrastructure to meet strict statutory and regulatory requirements governing the handling of PHI. With its increased enforcement and auditing, as well as increased scope, HIPAA compliance needs to be addressed as a matter of priority.

IN THIS WHITEPAPER

Offering a detailed overview of HIPAA and the key elements of HIPAA compliance, we examine the privacy, security, and breach notification considerations that organisations and their partners must meet. We then delve further into the HIPAA compliance framework, including the security standards, technical, administrative and physical safeguards. Also highlighted are the benefits of working with HIPAA-compliant partners such as CSPs.

2.0 ESSENTIALS OF HIPAA COMPLIANCE

The details that matter most

The Health Insurance Portability and Accountability Act (HIPAA) legislation was designed to make it easier for workers to retain health insurance coverage when they were between jobs. The Act also sought to drive the adoption of electronic health records to improve the efficiency and quality of the American healthcare system through improved information sharing.

First notified in 1996, HIPAA was considerably strengthened by the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009. This introduced breach notifications and significantly increased the penalties for HIPAA violations to a maximum of USD $1.5 million, giving HIPAA more bite than before. The final strengthening of HIPAA was completed in 2013, by expanding coverage to business associates of healthcare providers and their subcontractors – firmly establishing federal standards to protect the security and privacy of an individual's PHI.

What is Protected Health Information (PHI)?

Protected Health Information is the definition used by HIPAA to specify the type of information that falls under its jurisdiction. PHI includes all information related to:

PHI also includes many common identifiers, such as name, address, birth date and Social Security number.

Who needs to be HIPAA compliant?

All individuals or organisations who handle PHI need to be HIPAA compliant. Organisations include:

- **Healthcare providers** – such as hospitals, nursing homes, clinics, pharmacies, doctors, psychologists etc.
- **Health plans** – including those offered through health insurance companies, health maintenance organisations, employer-sponsored health initiatives, and Government programmes that pay for healthcare such as Medicare.
- **Healthcare clearinghouses** – include all organisations that process non-standard health information such as billing services.

These organisations are called ‘covered entities’.

What’s more, any organisation providing services to a covered entity is termed a ‘Business Associate’ (BA) and is equally expected to meet HIPAA requirements. Business associates include – but are not limited to – providers of internet technology, cloud services, software, financial services, legal services and business services.

HIPAA category breakdown

HIPAA Privacy Rule

The first federal information privacy law, finalised in 2000. This rule set a minimum standard for the protection of health information and privacy rights for U.S. citizens.

HIPAA Security Rule

Established in 2003 to notify physical, technical and administrative safeguards for electronic transactions of Protected Health Information (PHI).

HIPAA Breach Notification Rule

A part of the 2009 HITECH Act, to strengthen HIPAA penalties, introduce the requirement of breach notifications and expand patient rights.

Businesses are required to adhere to the HIPAA Privacy Rule and the HIPAA Security Rule to maintain the sanctity of PHI. Additionally, businesses must provide the appropriate notifications following a breach of unsecured PHI.

Understanding the HIPAA Privacy Rule

Healthcare organisations are entrusted with some of the most intimate and personal information over a patient's lifetime — relating to bank accounts and identity, as well as health. Patients expect that their data will be kept private. When that trust is breached, the ramifications for the healthcare organisation can be massive.

The HIPAA Privacy Rule seeks to protect a patient's private and personal health information. It sets safeguards, limits and conditions on the use and disclosure of PHI without patient authorisation. It also gives patients rights over their health information, including the right to examine and obtain a copy of their health records and request corrections. Business associates are directly liable for uses and disclosures of PHI that are covered under their Business Associates Agreement (BAA) or the HIPAA Privacy Rule. The Privacy Rule requires business associates to do the following:

- Disallow impermissible use or disclosures of PHI
- Notify covered entity of breaches
- Provide covered entity or individual access to PHI
- Disclose PHI to the Secretary of Health and Human Services (HHS), when asked
- Provide an accounting of disclosures
- Comply with all requirements of the HIPAA Security Rule

Understanding the HIPAA Security Rule

The HIPAA Security Rule was enacted to ensure that PHI is adequately protected and secure. Organisations must implement appropriate solutions and policies to comply with HIPAA security standards.

The HIPAA Security Rule requires covered entities to implement security measures to protect PHI. Patient health information must only be available to authorised users, and never improperly accessed or used. There are three types of safeguards needed:

Types of safeguards

Technical | Physical | Administrative

Requirement	Solution
Security management processes	• Perform a risk assessment to determine where the use of PHI, its storage and vulnerabilities could result in violations of HIPAA • Design and implement necessary measures to mitigate/reduce risks to appropriate levels • Implement sanction policies for employees who fail to comply with security policies and procedures • Regular review system logs, activities, audit trails etc.
Assigned security responsibility	• Designate HIPAA security and privacy officers
Workforce security	• Supervise employees who work with PHI, including authorisation and termination of access
Information access management	• Prevent unauthorised access to PHI by the parent company, partner companies and subcontracters • Implement procedures and maintain documentation for granting access to PHI
Security awareness and training	• Guard and report malicious software • Monitor logins and provide regular training to employees with PHI access • Implement password policies and procedures
Security incident procedures	• Identify, document and respond to security incidents
Contingency plan	• Make backups of all PHI and implement a process for its continued protection and critical business continuity during emergencies
Evaluations	• Perform periodic evaluations to assess continued HIPAA compliance procedures
Business associate contracts	• Sign agreements with partners to ensure they follow HIPAA

HIPAA Breach Notification Rule essentials

Despite the best efforts of healthcare organisations, breaches do occur and PHI is compromised. The Breach Notification Rule was brought about to notify the people affected by such a breach.

The Breach Notification Rule requires HIPAA-covered entities and their business associates to provide notification to the U.S. Department of Health and Human Services (HHS) following a breach of unsecured PHI. If the breach affects more than 500 patients, notification to the media and public is mandatory.

Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third party service providers, under the HITECH Act. Covered entities and business associates must demonstrate that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach.

In the event of an impermissible use or disclosure, a covered entity or business associate should maintain documentation to show that all required notifications were made or, conversely, were not required.

Covered entities must comply with certain administrative requirements concerning breach notification. For example, covered entities must have established written policies and procedures regarding breach notification, and must train employees on these policies and procedures. They are also obliged to develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

However, unintentional acquisition or inadvertent disclosure of PHI in good faith, and within the scope of authority without further use, are notable exceptions to the rule.

Penalties for HIPAA breaches

The HHS Office for Civil Rights enforces the HIPAA Privacy, Security and Breach Notification Rules – violations of which may result in civil monetary penalties. In certain, more severe cases, the U.S. Department of Justice may apply criminal penalties.

Common non-compliance issues include:
• Impermissible PHI uses and disclosures
• Lack of PHI safeguards
• Lack of patient access to PHI
• Use or disclosure of more than the minimum necessary PHI
• Lack of administrative PHI safeguards

HIPAA violations can prove highly costly for organisations and their partners. The fines for noncompliance are based on the level of perceived negligence found within your organisation at the time of the HIPAA violation. These fines can range from USD $100 to USD $50,000 per violation (or per record), with a maximum penalty of USD $1.5 million per year for each violation. To date, penalties amounting to more than USD $75 million have been levied in 53 cases of violation.[3]

The tiered penalty system reflects the gravity of each violation.

	For violations occuring proir to 2/18/2009	For violations occuring on or after 2/18/2009
Penalty amount	Up to **$100** per violation	**$100** to **$50,000** or more per violation
Calender year cap	**$25,000**	**$1,500,000**

Source - https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

For the healthcare industry, ironclad data protection is always a priority. Couple this with the deployment of technology accelerators such as the Internet of Things (IoT) and Artificial Intelligence (AI). As both rapidly become the norm, they show that healthcare organisations need to stay both connected and protected.

While the advancement of technology is exciting in itself, it's also creating new capabilities for healthcare organisations to treat patients, access and share data, as well as communicate with patients and staff in real time via connected devices. To enable these technologies, organisations are working with partners around the world. Data is therefore continuously moving between devices, partners and entities – creating creating a higher risk profile than before.

To mitigate these risks, healthcare organisations need partners who are HIPAA compliant. Any partner worth considering must have undergone successful audits for HIPAA compliance. A compliant, knowledgeable partner goes a long way towards reducing risk.

Exceptions to HIPAA requirements

In certain cases, when health information is collected in the course of a study, it is possible to use this information for research purposes without the an individual's authorisation. However, in such a case the records should be de-identified and modified to limited data sets, i.e. exclude all direct identifiers of the individual.

3.0 THE CAPABILITIES OF HIPAA-COMPLIANT PARTNERS

How they can be a catalyst for your business

HIPAA compliance is central to the future of the healthcare industry and your organisation's place in it. Beyond the hefty cost of a HIPAA violation, the irreversible damage to your organisation's reputation could be even more devastating. What's more, an increasing number of healthcare providers have started ensuring HIPAA compliance and are limiting themselves to working with HIPAA-compliant partners. This allows organisations to alleviate stress and reduce operating costs. A prospective partner – a managed hosting provider or network partner for example – must exceed both the physical and digital security standards needed to safeguard PHI.

Here's a helpful checklist to help you choose the right HIPAA-compliant partner:

1. Advanced auditing

Your partners must conform to HIPAA regulations confirmed through audits to guarantee your data is secure and fully HIPAA compliant.

2. Business associate agreement (BAA)

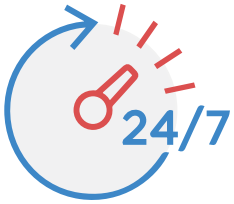
The hosting partner must provide you with a BAA that protects your organisation. A BAA establishes a clear line of responsibility concerning your data security and the liability of your partner.

3. Certifications

The right partner needs to maintain and work towards increasing their level of certifications. All their employees must be HIPAA certified, and always request validation of their certification and third-party audits.

4. Experience

An appropriate partner must have extensive experience working within the healthcare industry and adapting to regulatory changes. Ask prospective partners for referrals from their current healthcare customers.

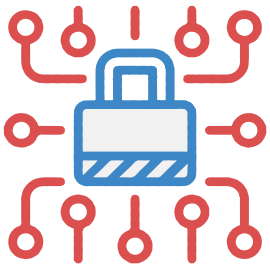


5. Single point support

A proactive partner must provide 24/7/365 support without complex escalation protocols. This is vital for remaining HIPAA compliant and resolving issues seamlessly.

6. Business continuity plan

Partners must anticipate a cyber-attack, natural disaster or any other possibility that may impact the availability or security of their systems. Enquire about their disaster recovery and business continuity plans. Find out what protocols and preventative measures they have in place to ensure the safety of your data.



7. Guaranteed SLAs

Beyond compliance, another important partner feature should be a guaranteed service level agreement. The healthcare industry requires fast, immediate access to information. When there is a patient in the room, providers can't afford to be delayed by downtime.

If your prospective partner meets these requirements, it's a positive indicator for them and your organisation.

4.0 OUR COMMITMENT TO HIPAA COMPLIANCE

Enabling your business to move forward

As the healthcare environment evolves to adhere to new requirements, organisations need partners with a comprehensive portfolio of managed technology services to boost connectivity and reliability, along with enhanced security solutions.

Tata Communications matches this partner profile exactly, helping healthcare organisations benefit from Managed Hosting Services (MHS) and Managed Security Services (MSS) by building the complete foundation for a well-defended digital healthcare landscape. While there is no HIPAA certification for MHS or MSS providers, Tata Communications has aligned itself with all HIPAA compliance tenets.

HIPAA-compliant services

Tata Communications delivers secure, compliant, highly accessible solutions that empower companies to increase revenues, reduce expenses and manage risk. Our solutions promote a more secure data environment and build higher assurance into compliance efforts.

We're HIPAA-compliant for all services provided by the Global Service Management Centre (GSMC) including MHS and MSS.

MHS and HIPAA-compliant services

- Managed Hosting (Server, Storage, Switch, Network Connectivity, Firewall)
- Managed Backup Service
- Managed Load Balancer Service
- Managed Database Management (DBA) Service
- Managed Virtual Host – Shared Virtualisation Service

MSS and HIPAA-compliant services

- Managed Authentication Service
- Managed Firewall and Unified Threat Management Service
- Managed Proxy Service
- Managed Intrusion Detection & Prevention Systems Service
- Managed Distributed Denial of Service – Detection & Mitigation Service
- Managed Virtual Unified Threat Management (Virtual Next-Generation Firewall) Service
- Managed Web Application Firewall Service

In-scope IDCs include

- LVSB, Mumbai, India
- VSB Chennai, India
- TCX Singapore
- UK Cressex
- US New York
- US Santa Clara

Tata Communications provides and manages the underlying infrastructure (operating systems, database and network devices, including providing certain value-added services such as managed backups). This supports the customer's applications or file servers, which may hold PHI. Tata Communications is entirely responsible for the management and administration of GSMC infrastructure.

However, the scope of the HIPAA Privacy Rule and Breach Notification Rule is restricted only to the extent of Tata Communications' service responsibilities.

Certifications

Tata Communications is ISO 27001:2013 & ISO 20000-1:2011 certified for the MHS and MSS services. Internal and external audits are conducted regularly to validate certifications.

Additionally, Tata Communications services are assessed for SSAE18/ ISAE3402 Type 2 on a yearly basis.

Risk assessment

Tata Communications carries out periodic risk assessments for its core infrastructure. The risk assessment covers both physical and logical risks. Quarterly reviews of the risk mitigation action for assessing the current risk value is in place.

Risk assessment of customer infrastructure managed by Tata Communications is a responsibility of the customer, as it is only they who can determine asset criticality. Additionally, the assessment scope does not cover risks related to stored PHI data or the application used for accessing it.

Business Associate Agreement (BAA)

Tata Communications has a standard BAA that accounts for our shared responsibility for HIPAA compliance.

Access control management

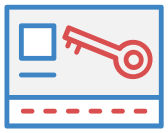
Access control management covers the entire core infrastructure and is reviewed quarterly. Physical access control management determines access control to the environment where the infrastructure is hosted.

Access control management responsibility for the customer devices resides with the customer, whether or not the customer takes Managed Services from Tata Communications.

Vulnerability assessment

Vulnerability assessment is carried out for the entire Tata Communications infrastructure, with respective teams responsible for mitigating risk-related findings.

Tata Communications also offers vulnerability assessment as a service for any customer's benefit. Vulnerability assessment frequency is based on the customer contract. The reports are shared with customers upon completion of vulnerability assessment, and action steps then recommended by Tata Communications to customers for remediation.



Limited access

Tata Communications ensures a minimum necessary access requirement, which states that only those who require PHI to fulfil their jobs should get access. Unless you have a specific and compelling need for the information, access must be restricted.

Disaster Recovery (DR) and Business Continuity Plan (BCP)

Tier III-rated, SAS SSAE 16 and HIPAA-certified data centres offer healthcare organisations fully redundant and highly secure facilities to host mission-critical applications and disaster recovery (DR) operations at a lower cost of ownership.

Our BCP ensures customers' healthcare systems remain fully operational 24/7/365. Also, our solutions are backed by industry-leading SLAs and always-on infrastructure management and support – mitigating time, cost and risk.

Security training

All Tata Communications employees must attend and complete information security awareness training which is updated every year for new developments.

Beyond Tata Communications' scope

The applicability of HIPAA controls shall not extend to classification or management of PHI. Additionally, Tata Communications' service responsibilities do not include management or review of PHI residing within the underlying infrastructure.

The encryption of data at rest and in transit falls under the responsibility of the customer storing or transmitting the data.

5.0 IN CONCLUSION

A compliant future for healthcare organisations

The healthcare industry is constantly evolving to meet federal requirements for electronic PHI maintenance, transmission and storage. Today's healthcare organisations are choosing HIPAA-compliant partners that reduce the risk of PHI breaches, lessen network complexity, offset capital costs and enhance network agility to deliver better patient care and healthcare service delivery at lower cost.

As these healthcare organisations integrate their data and business structures in the virtual space, they need to continually invest in hardware-enhanced security technologies and software solutions that protect identities, data and infrastructure. Someone from the C-Suite needs to believe in the inherent benefits of HIPAA, not only for mandatory compliance but also as a positive influence to improve the customer experience and enhance brand value.

Healthcare organisations and their partners need to develop best practices, standards and governance models to ensure HIPAA-compliant processes and policies are built into their operational models, rather than being a mere afterthought.

Tata Communications' HIPAA-compliant MHS and MSS solutions empower healthcare institutions and providers to focus on their business and patient care, rather than spending extra time, effort and resources worrying about compliant IT services. We fully understand the challenges of securing PHI and other specific HIPAA-related requirements.

SOURCES

- Source 1 - https://www.reportlinker.com/p05251939/Healthcare-Cloud-Computing-Global-Markets-to.html
- Source 2 - https://www.hipaajournal.com/largest-healthcare-data-breaches-2017/
- Source 3 - https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

For more information, visit us at **www.tatacommunications.com**

CONTACT US

©2018 Tata Communications. All rights reserved.
TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Limited in certain countries