# HIPAA COMPLIANCE
# MICROSOFT OFFICE 365 AND MICROSOFT TEAMS

Microsoft HIPAA One PROTECT YOUR ePHI

- April 2019 -

## Contributors

**_Steven Marco, CISA_**
Founder & CEO
HIPAA One

**_Bobby Seegmiller_**
Executive VP
HIPAA One

**_John Lazo, CISM CISA_**
VP, Data Security
HIPAA One

**_Garrett Hall, JD_**
VP, Strategy
HIPAA One

**_Arch Beard_**
InfoSec Officer,
Adventist Health

Microsoft

HIPAA One
PROTECT YOUR ePHI

## About the Authors

This whitepaper was prepared for Microsoft, created by HIPAA One, with the support of Microsoft's Product teams. HIPAA One is the leading HIPAA Compliance Software and Services firm in the United States. Since its inception in 2012, HIPAA One has collected HIPAA compliance data for over 6,000 locations and audited thousands of healthcare organizations. HIPAA One employs a team of in-house certified Auditors/Security Practitioners and recently integrated their software with some of the nation's largest electronic medical record companies such as athenahealth and Allscripts. HIPAA One aims to simplify HIPAA compliance through use of their automated, cloud-based software.

***Disclaimer:*** *This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice and are solely those of HIPAA One and not Microsoft Corporation. You bear the risk of using it.*

## Contents

# EXECUTIVE SUMMARY

This document provides healthcare executives, management and administrative teams the necessary information to satisfy HIPAA compliance and cybersecurity diligence using Microsoft Office 365 ("Office 365") and Microsoft Teams ("Teams"). By implementing the controls found in this whitepaper, healthcare organizations may significantly reduce the likelihood of breaches while working towards meeting US and Global regulatory standards such as HIPAA, GDPR, new and evolving consumer privacy laws[1] and HITRUST Certification requirements.

In this digital age, anyone with an internet connection is a target for fraud. Due to the nature of sensitive protected health information and personally identifiable information, healthcare providers have increasingly complex fraud challenges and cybersecurity workforce issues. Without taking action to implement data security, given enough time, the chances of being breached becomes 100%.

A recent annual survey from A.T. Kearney of 400 C-level executives and board members from around the world revealed that more than 85% reported experiencing a breach in the past three years and they ranked business disruption from cybersecurity risks as their no.1 business challenge. Despite that staggering statistic, only 39% said their company has fully developed and implemented a cyber defense strategy, putting the 61% of respondents at increased risk for future attacks[2].

Implementing a HIPAA compliance and cyber defense strategy is mandatory for all healthcare organizations and their business associates. While building a foundation of compliance, the HIPAA Security Risk Analysis requirement per 164.308(a)(1)(ii)(A) along with NIST-based methodologies[3] are critical tools for audit scenarios and data security. As described in Part 2, Microsoft built all its cloud applications and networks following its own Trusted Cloud principles for security, privacy and compliance. By doing so, Microsoft recently achieved compliance with the HIPAA Security Rule, HITRUST Certification in Azure and Office 365 along with dozens of other global, regional, industry and US Government certifications[4].

Thanks to heavy investments Microsoft has made in security, compliance and auditing; anyone who utilizes data should also read the following whitepaper. Specifically, Office 365 and Teams users can leverage built-in security and compliance features documented in Part 3 to combat the constantly evolving cyber-security attacks everyone faces in healthcare and beyond.

The following whitepaper consists of three sections and appendices containing relevant guidance and/or illustrations intended to demonstrate how to leverage Office 365 and Teams to achieve compliance for each aspect of the HIPAA Security Rule.

[1] California and other similar states have implemented their own security and consumer privacy laws which are enacted or pending.

[2] Rising to the Challenge-2018 Views from C-Suite, A.T. Kerny, Paul Laudicina; Courtney Rickert McCaffrey; Erik Peterson, October 16, 2018

[3] The National Institute of Standard and Technology (NIST) is the US Government Department who issues Federal cybersecurity and data security standards. They issue special publications which highlight methodologies the entire data security industry follows.

[4] Microsoft Cloud Architecture Security, Brenda Carter, Microsoft December 4, 2018.

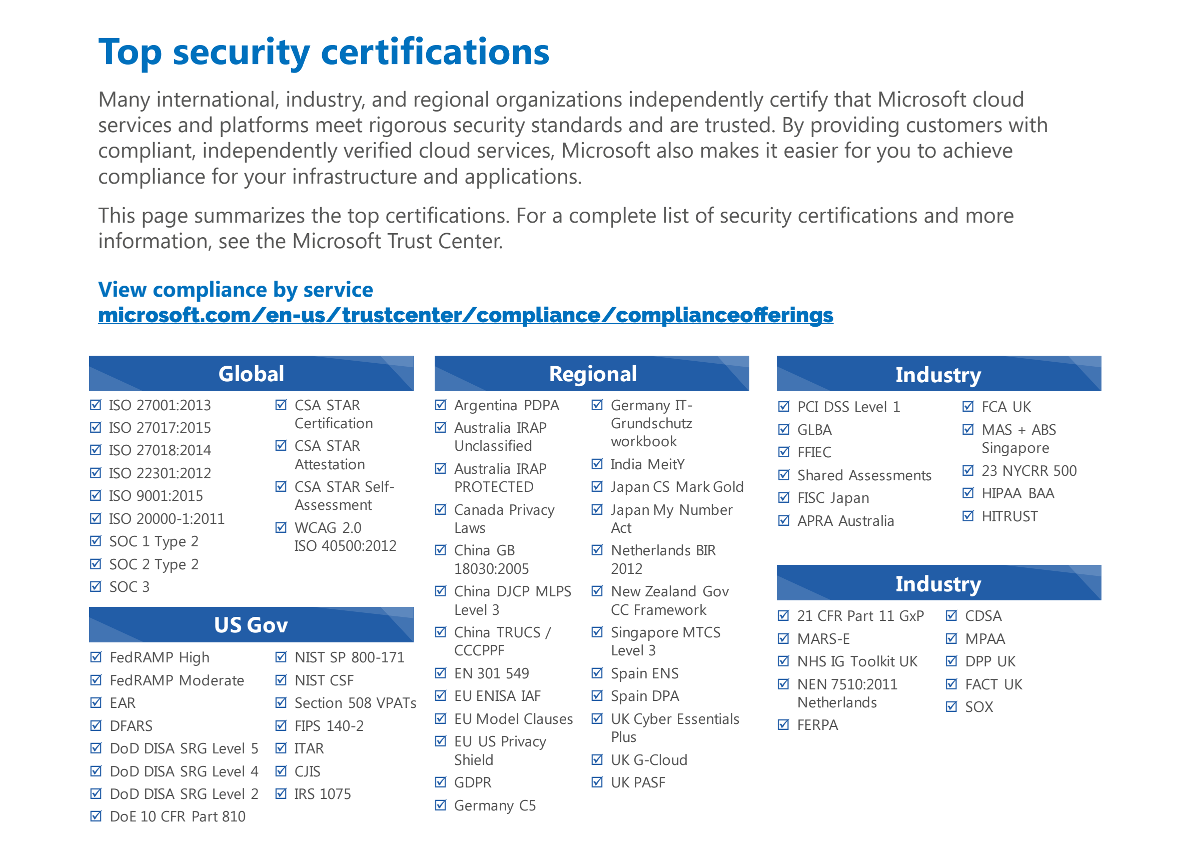
Part 1

# UPDATES TO HIPAA REGULATIONS AND GDPR

CIOs, IT Directors and IT Managers are often deputized as their organization's Health Insurance Portability and Accountability Act (HIPAA) Security Officer. In addition to being responsible for HIPAA security and compliance, these individuals may also be tasked with overseeing a company-wide migration to cloud services, namely migrating to Office 365.

Organizations in every industry, including many US government agencies, are upgrading to Office 365 to improve their security posture. Office 365 and Teams has been designed to be the most secure cloud platform yet with architectural advancements built into every layer of the cloud's stack. However, as with all software upgrades, functionality, security and privacy implications must be understood and addressed.  As mentioned above, sending data to the cloud requires HIPAA Security Officers to ask the key question: ***"How does Office 365 and using Teams enable me to meet or exceed our HIPAA Security and Privacy requirement in my environment?"***

Microsoft has put tremendous focus in the area of security and has the following global, regional, US and industry certifications[5]:



## Top security certifications

Many international, industry, and regional organizations independently certify that Microsoft cloud services and platforms meet rigorous security standards and are trusted. By providing customers with compliant, independently verified cloud services, Microsoft also makes it easier for you to achieve compliance for your infrastructure and applications.

This page summarizes the top certifications. For a complete list of security certifications and more information, see the Microsoft Trust Center.

**View compliance by service**
**microsoft.com/en-us/trustcenter/compliance/complianceofferings**

### Global

☑ ISO 27001:2013
☑ ISO 27017:2015
☑ ISO 27018:2014
☑ ISO 22301:2012
☑ ISO 9001:2015
☑ ISO 20000-1:2011
☑ SOC 1 Type 2
☑ SOC 2 Type 2
☑ SOC 3
☑ CSA STAR Certification
☑ CSA STAR Attestation
☑ CSA STAR Self-Assessment
☑ WCAG 2.0 ISO 40500:2012

### US Gov

☑ FedRAMP High
☑ FedRAMP Moderate
☑ EAR
☑ DFARS
☑ DoD DISA SRG Level 5
☑ DoD DISA SRG Level 4
☑ DoD DISA SRG Level 2
☑ DoE 10 CFR Part 810
☑ NIST SP 800-171
☑ NIST CSF
☑ Section 508 VPATs
☑ FIPS 140-2
☑ ITAR
☑ CJIS
☑ IRS 1075

### Regional

☑ Argentina PDPA
☑ Australia IRAP Unclassified
☑ Australia IRAP PROTECTED
☑ Canada Privacy Laws
☑ China GB 18030:2005
☑ China DJCP MLPS Level 3
☑ China TRUCS / CCCPPF
☑ EN 301 549
☑ EU ENISA IAF
☑ EU Model Clauses
☑ EU US Privacy Shield
☑ GDPR
☑ Germany C5
☑ Germany IT-Grundschutz workbook
☑ India MeitY
☑ Japan CS Mark Gold
☑ Japan My Number Act
☑ Netherlands BIR 2012
☑ New Zealand Gov CC Framework
☑ Singapore MTCS Level 3
☑ Spain ENS
☑ Spain DPA
☑ UK Cyber Essentials Plus
☑ UK G-Cloud
☑ UK PASF

### Industry

☑ PCI DSS Level 1
☑ GLBA
☑ FFIEC
☑ Shared Assessments
☑ FISC Japan
☑ APRA Australia
☑ FCA UK
☑ MAS + ABS Singapore
☑ 23 NYCRR 500
☑ HIPAA BAA
☑ HITRUST

### Industry

☑ 21 CFR Part 11 GxP
☑ MARS-E
☑ NHS IG Toolkit UK
☑ NEN 7510:2011 Netherlands
☑ FERPA
☑ CDSA
☑ MPAA
☑ DPP UK
☑ FACT UK
☑ SOX

[5] Microsoft Cloud Architecture Security, Brenda Carter, Microsoft December 4, 2018

A common concern in the healthcare industry is that using Office 365 and Teams exposes an organization to HIPAA violations. The truth is Office 365 and Teams can be easily configured to support HIPAA security and privacy requirements. **This whitepaper outlines such configurations and will review the bigger-picture cloud features, as applicable in an over-arching security architecture:**

## Challenges facing health organizations

**Enhanced mobility and collaboration**

Increased threat exposure Greater risk Evolving threats

**Data leaks and targeted attacks**

Increased costs
Out-of-date defenses
Eroding patient trust

**Compliance regulations**

Increased scrutiny
Complex regulations
Legal implications

**The HIPAA Privacy Rule, at a high level, ensures individuals have the minimum protections under the law. Incorrect configuration of modern operating systems, including Office 365, could violate the following laws and may lead to HIPAA non-compliance:**

- **Access to the Health Record**
  See §164.524, §164.526
- **Minimum Necessary Uses of PHI**
  See § 164.502(b), § 164.514(d)
- **Content and Right to an Accounting of Disclosures**
  See §164.528
- **Business Associate Contracts**
  ee § 164.504(e)[6]

A key component of HIPAA compliance today is the demonstration of appropriate IT-related internal controls designed to mitigate fraud and risk; and the implementation of safeguards for legally protected health information. All users accessing this information are also required to meet IT compliance standards. Written from an auditor's perspective, this whitepaper addresses the area of Office 365 Enterprise IT Security compliance for HIPAA.

[6] Visit https://www.govinfo.gov for individual Code of Federal Regulations and HIPAA Citations

**Specifically, the HIPAA Security Rule requires healthcare organizations to:**

1 Ensure the confidentiality, integrity, and availability of all electronic protected health information ("ePHI") created, received, maintained, or transmitted

2 Regularly review system activity records, such as audit logs, access reports, and security incident tracking reports

3 Establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process containing ePHI

4 Monitor login attempts and report discrepancies

5 Identify, respond to and document security incidents

6 Obtain satisfactory assurances from their vendors before exchanging ePHI (i.e. Business Associates)

A new regulation has begun popping up within the healthcare technology community and has gained tremendous momentum in the way of media coverage and industry articles. If you've heard the term General Data Protection Regulation recently and did not understand what it was referring to, know that you're not alone. In March of 2018, HIPAA One conducted a webinar poll with over 300 registrants and found that 81% of Providers did not know what GDPR was referring to, let alone its potential impact on the U.S. healthcare industry.

The ***General Data Protection Regulation*** ("GDPR") is a data protection law in the European Union ("EU") and the European Economic Area ("EEA") that gives individuals control over their data and provides data protection, globally. The law also requires organizations to bolster their privacy and data protection measures and imposes significant penalties and fines up to the greater of €20 million or 4% of annual global revenue for those who violated its provisions.

***How will this framework impact U.S. based healthcare providers?*** U.S. companies do not need to have business operations in one of the 28-member states of the European Union to be impacted by GDPR. GDPR requires all organizations who process EU/EEA residents' data to support a high level of privacy protection and account for where that data is stored.

GDPR only applies to organizations that are considered "established" in the EU. Being "established" in the EU does not necessary require the physical presence of a corporate entity. Rather, an organization is "established" to the extent that it exercises "effective and real" activity in the EU, and processes personal data in the context of those activities, through "stable arrangements." The legal form of those arrangements is not determinative and could be met by the presence of an employee or agent." Even in circumstances where a US company engages in no activities that would render it established in the EU, it can still be subject to GDPR if it offers goods or services to EU data subjects or monitors the behavior of EU data subjects within the EU. GDPR is not triggered simply because a US company offers goods or services to EU data subjects.

GDPR replaces the Data Protection Directive (adopted in 1995) which had previously been the basis for protecting personal data in the EU. The Data Protection Directive, however, did not by itself govern all member states of the EU. Each member country had to adopt the Directive into law which all EU member states did, but with slight variations for each state. GDPR replaces the Data Protection Directive and is binding and enforceable on all member states and companies that conduct business in the EEA.

The GDPR consists of 99 articles with an additional 171 recitals with explanatory remarks. A few of the key requirements of the GDPR include:

- Requiring a legal basis for data processing
- Notifying the supervisory authorities “without undue delay" but not later than 72 hours after discovering a breach
- Following certain requirements if there are cross-border transfers of personal data
- Appointing a Data Protection Officer ("DPO") is required by GDPR of companies in certain instances

GDPR is having an impact on data protection requirements globally. In January of 2019, Google was fined €50 million for failing to adequately inform users about their data collection practices, and not giving users enough control over how their information is used. This appears to only be the beginning. Understanding, and adhering to, GDPR should be of utmost importance to companies doing business in the EEA.

The below table provides a summary comparing breach notification requirements under HIPAA and GDPR:

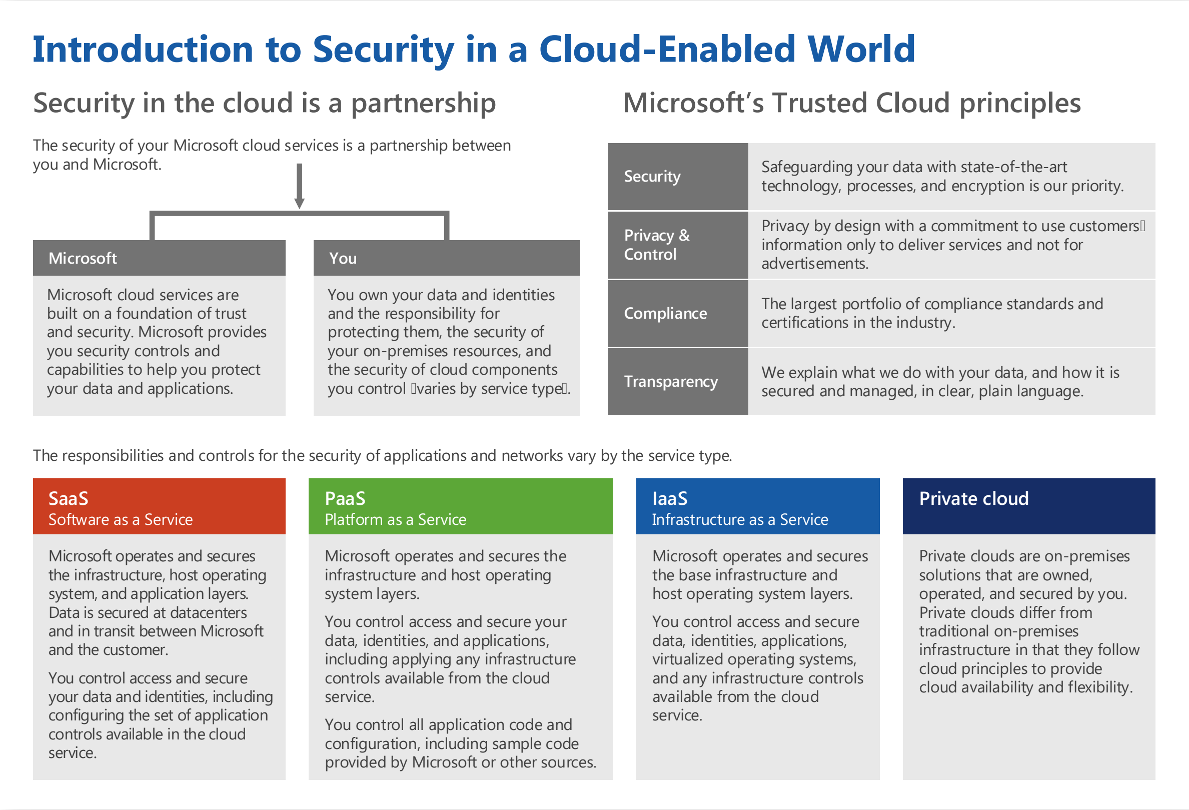
| | HIPAA | GDPR |
|---|---|---|
| **Covered Information** | PHI is defined as information about an individual's health care, created, received or maintained by a health care provider, that identifies an individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information related to the past, present or future physical or mental health or condition of an individual; information about the provision of health care to an individual; and information related to the past, present or future payment for the provision of health care to an individual." | "Personal data," is defined as any information relating to an identified or identifiable natural person who is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| **A breach occurs when…** | Generally, there is an acquisition, access, use, or disclosure of PHI not permitted under the Privacy Rule. | There is "the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed." |
| **Harm Threshold** | An acquisition, access, use, or disclosure of PHI not permitted under the Privacy Rule. Exceptions apply.[7] | With respect to notification to supervisory authorities, the test is whether the breach is likely to result in "a risk to the rights and freedoms of natural persons."<br>With respect to consumer notification, the test is whether the breach is likely to result in "a high risk to the rights and freedoms of natural persons." |
| **Notification Requirements (Regulatory)** | **Timing:** To individuals without unreasonable delay and no later than 60 calendar days after discovery of the breach. For breaches affecting 500 or more individuals, to HHS and the media without unreasonable delay and no later than 60 calendar days after discovery of the breach. For breaches affecting less than 500 individuals, to HHS within 60 days after the end of the calendar year during which the breach occurred.<br>**Content:** In plain language and including date of the breach and date of discovery of the breach, description of the types of information involved, steps individuals should take to protect themselves, description of the corrective action taken in response to the breach and entity contact procedures."<br>**Method:** First class mail or email, if the individual has agreed to receive electronic notice." | **Timing:** "Without undue delay."<br>**Content:** A description "in clear and plain language" of the nature of the breach and items (2)-(4) of the regulatory notification.<br>**Method:** May be done via a public communication or similar measure if providing the communication to the data subjects directly would involve disproportionate effort. |

[7] The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

Part 2

# MICROSOFT’S OFFICE 365 AND TEAMS: DATA SECURITY AND HIPAA COMPLIANCE

With the constantly-evolving proliferation of information security threats, mixed with the complexity of meeting HIPAA regulatory mandates, healthcare organizations today need as many built-in compliance and security features as possible. The Microsoft Office 365 Information Protection suite provide organizations integrated, turn-key security controls not previously available. Never before has it been easier to meet many of the technical and administrative safeguards required by today’s HIPAA Security mandates while also enabling modern cyber-security controls. For example, Data Loss Prevention, Security Incident Event Management, data classification and encryption for data-at-rest recently were only achievable leveraging separate, expensive, off-the shelf vendors, and now are centrally built-in when using Microsoft’s Cloud services.



## Introduction to Security in a Cloud-Enabled World

### Security in the cloud is a partnership

The security of your Microsoft cloud services is a partnership between you and Microsoft.

| Microsoft | You |
|---|---|
| Microsoft cloud services are built on a foundation of trust and security. Microsoft provides you security controls and capabilities to help you protect your data and applications. | You own your data and identities and the responsibility for protecting them, the security of your on-premises resources, and the security of cloud components you control varies by service type. |

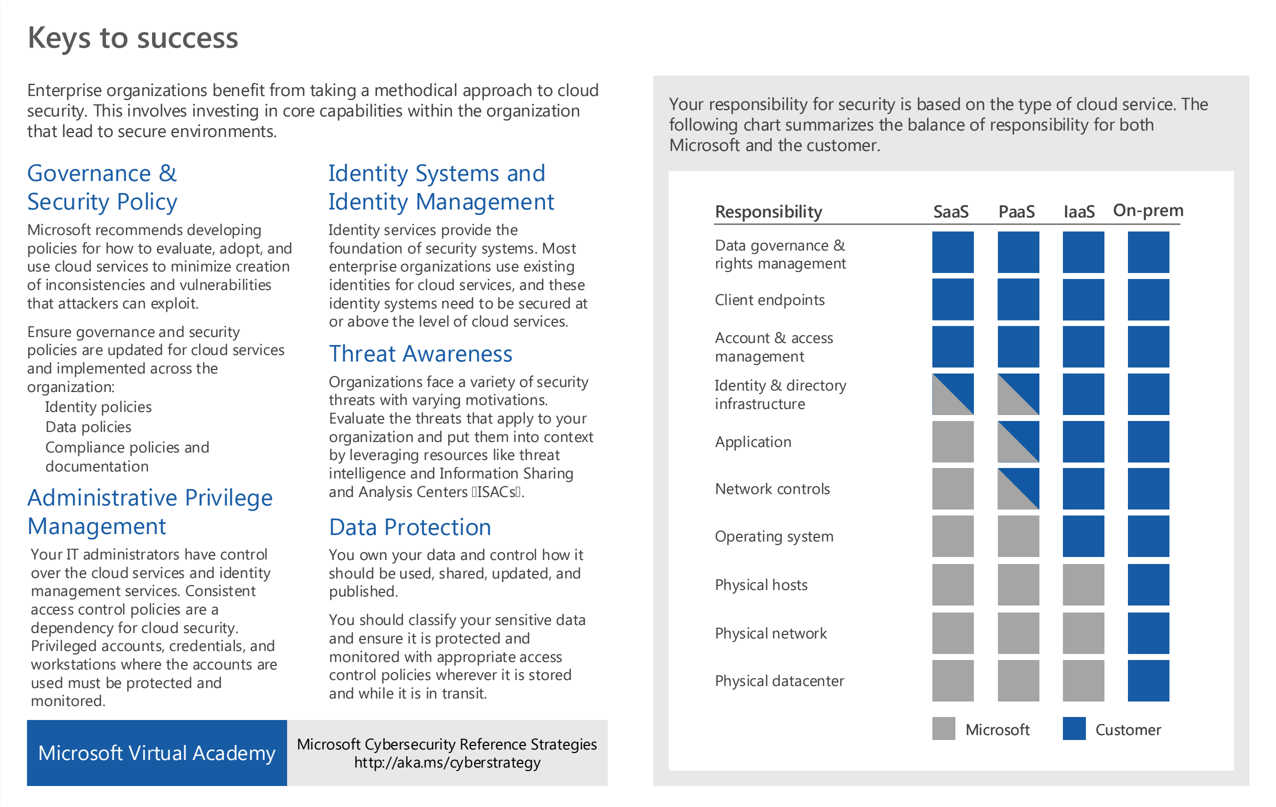
### Microsoft’s Trusted Cloud principles

| | |
|---|---|
| Security | Safeguarding your data with state-of-the-art technology, processes, and encryption is our priority. |
| Privacy & Control | Privacy by design with a commitment to use customers information only to deliver services and not for advertisements. |
| Compliance | The largest portfolio of compliance standards and certifications in the industry. |
| Transparency | We explain what we do with your data, and how it is secured and managed, in clear, plain language. |

The responsibilities and controls for the security of applications and networks vary by the service type.

| SaaS<br>Software as a Service | PaaS<br>Platform as a Service | IaaS<br>Infrastructure as a Service | Private cloud |
|---|---|---|---|
| Microsoft operates and secures the infrastructure, host operating system, and application layers. Data is secured at datacenters and in transit between Microsoft and the customer.<br>You control access and secure your data and identities, including configuring the set of application controls available in the cloud service. | Microsoft operates and secures the infrastructure and host operating system layers.<br>You control access and secure your data, identities, and applications, including applying any infrastructure controls available from the cloud service.<br>You control all application code and configuration, including sample code provided by Microsoft or other sources. | Microsoft operates and secures the base infrastructure and host operating system layers.<br>You control access and secure data, identities, applications, virtualized operating systems, and any infrastructure controls available from the cloud service. | Private clouds are on-premises solutions that are owned, operated, and secured by you. Private clouds differ from traditional on-premises infrastructure in that they follow cloud principles to provide cloud availability and flexibility. |

Although Office 365 has integrated these functions together providing clear lines of delineation between Microsoft and customer responsibilities to support customer's HIPAA and GDPR compliance, HITRUST Certification, and many other regulatory mandates, the focus of this whitepaper is compliance with HIPAA. Thanks to Microsoft, investments made implementing HIPAA from this whitepaper can be re-used to comply with numerous global standards and mandates in security controls[8]. Microsoft Teams is a unified communications platform that combines persistent workplace chat, video meetings, file storage, and application integration. The service integrates with the company's Security and Compliance Office 365 subscription office productivity suite and features extensions that can integrate with non-Microsoft products.



## Keys to success

Enterprise organizations benefit from taking a methodical approach to cloud security. This involves investing in core capabilities within the organization that lead to secure environments.

### Governance & Security Policy

Microsoft recommends developing policies for how to evaluate, adopt, and use cloud services to minimize creation of inconsistencies and vulnerabilities that attackers can exploit.

Ensure governance and security policies are updated for cloud services and implemented across the organization:

- Identity policies
- Data policies
- Compliance policies and documentation

### Administrative Privilege Management

Your IT administrators have control over the cloud services and identity management services. Consistent access control policies are a dependency for cloud security. Privileged accounts, credentials, and workstations where the accounts are used must be protected and monitored.

### Identity Systems and Identity Management

Identity services provide the foundation of security systems. Most enterprise organizations use existing identities for cloud services, and these identity systems need to be secured at or above the level of cloud services.

### Threat Awareness

Organizations face a variety of security threats with varying motivations. Evaluate the threats that apply to your organization and put them into context by leveraging resources like threat intelligence and Information Sharing and Analysis Centers ISACs.

### Data Protection

You own your data and control how it should be used, shared, updated, and published.

You should classify your sensitive data and ensure it is protected and monitored with appropriate access control policies wherever it is stored and while it is in transit.

Microsoft Virtual Academy

Microsoft Cybersecurity Reference Strategies
http://aka.ms/cyberstrategy

Your responsibility for security is based on the type of cloud service. The following chart summarizes the balance of responsibility for both Microsoft and the customer.

| Responsibility | SaaS | PaaS | IaaS | On-prem |
|---|---|---|---|---|
| Data governance & rights management | 🟦 | 🟦 | 🟦 | 🟦 |
| Client endpoints | 🟦 | 🟦 | 🟦 | 🟦 |
| Account & access management | 🟦 | 🟦 | 🟦 | 🟦 |
| Identity & directory infrastructure | ◩ | ◩ | 🟦 | 🟦 |
| Application | ⬜ | ◩ | 🟦 | 🟦 |
| Network controls | ⬜ | ◩ | 🟦 | 🟦 |
| Operating system | ⬜ | ⬜ | 🟦 | 🟦 |
| Physical hosts | ⬜ | ⬜ | ⬜ | 🟦 |
| Physical network | ⬜ | ⬜ | ⬜ | 🟦 |
| Physical datacenter | ⬜ | ⬜ | ⬜ | 🟦 |

⬜ Microsoft 🟦 Customer

[8] Microsoft Cloud Architecture Security, Brenda Carter, Microsoft December 4, 2018

| | | Business Essentials & Business Premium | Microsoft 365 Business | Office 365 Enterprise E3 | Microsoft 365 Enterprise E3 | Office 365 Enterprise E5 | **Microsoft 365 Enterprise E5** | Price |
|---|---|---|---|---|---|---|---|---|
| Security | Advanced Threat Protection | Add-on | Add-on | Add-on | Add-on | Included | Included | $2 |
| | Advanced Security Management | Add-on | Add-on | Add-on | Add-on | Included | Included | $3 |
| | Advanced Compliance | Add-on | Add-on | Add-on | Add-on | Included | Included | $8 |
| | Threat Intelligence | Add-on | Add-on | Add-on | Add-on | Included | Included | $8 |
| Analytics | MyAnalytics | Add-on | Add-on | Add-on | Add-on | Included | Included | $4 |
| | Power BI Pro | Add-on | Add-on | Add-on | Add-on | Included | Included | $10 |
| Voice | PSTN Canferencing | Add-on | Add-on | Add-on | Add-on | Included | Included | $4 |
| | Cloud PBX | N/A | N/A | Add-on | Add-on | Included | Included | $8 |
| | PSTN Calling ▯US Only▯ | N/A | N/A | Add-on<br>Cloud PBX Required | Add-on<br>Cloud PBX Required | Add-on | Add-on | $12/$24** |

**All these capabilities are designed to provide additional controls for protecting, detecting and reducing the likelihood of data breaches.**

The subscription used to perform evaluations and testing in this whitepaper is Microsoft Teams within the Office 365 E5 suite.  This suite provides the maximum number of features for HIPAA configuration for an organization.

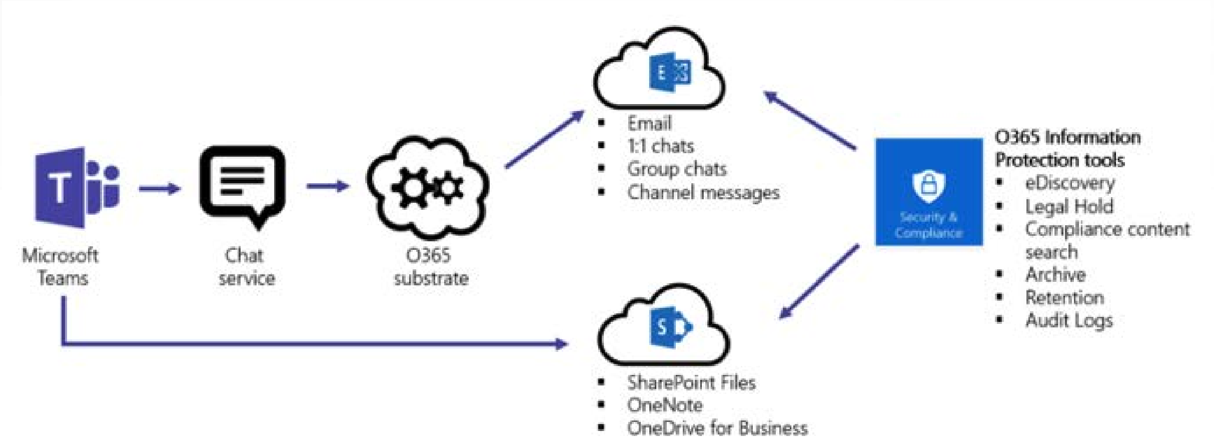
## Security and Compliance for Office 365 and Teams

By leveraging Microsoft's Trusted Cloud principles, organizations can achieve some quick HIPAA security and compliance wins in Office 365 and Teams. Per at Microsoft's security roadmap, the following features of the Microsoft cloud are available with Office E5 licensing:

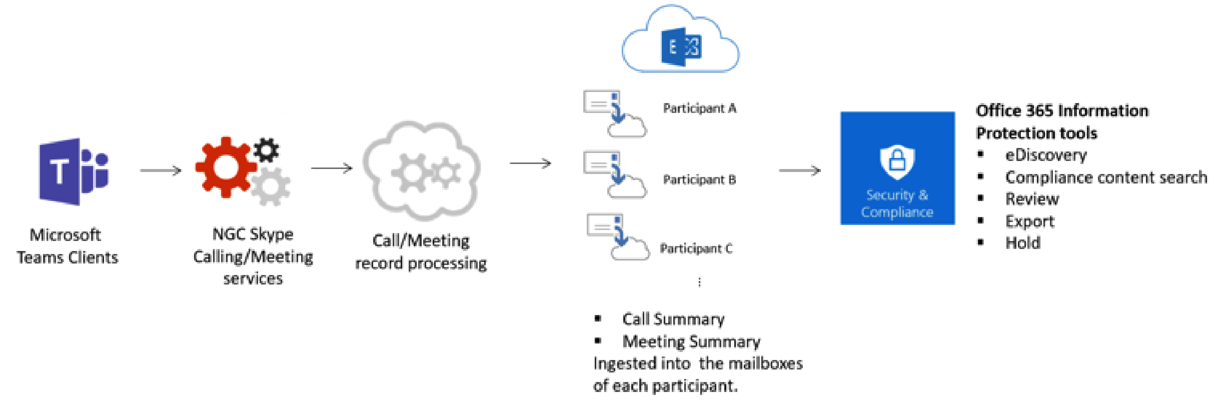
1. Exchange e-mail gateway/anti-malware services called Office 365 Advance Threat Protection (ATP)
2. Windows Defender with Advance Threat Protection (WATP)
3. Cloud App Security (CAS)
4. Azure AD Identity Protection
5. Azure Security Center
6. Azure Advance Threat Protection
7. Log Analytics workspace
8. Mobile Application Management, Windows Information Protection and Mobile Device Management

**Office 365 Information Protection controls Exchange and SharePoint for Teams files, messages, calls and meetings as these tools are integrated into Microsoft's cloud stack architecture.**

Security and Compliance personnel can centrally manage information protection tools and HIPAA Security controls in Office 365 as all application data flows through Office 365 as illustrated below:



Teams meetings and calling data to Exchange are also controlled centrally by Office 365:


Microsoft Teams Clients
NGC Skype Calling/Meeting services
Call/Meeting record processing
Participant A
Participant B
Participant C
Call Summary
Meeting Summary
Ingested into the mailboxes of each participant.
Security & Compliance
Office 365 Information Protection tools
eDiscovery
Compliance content search
Review
Export
Hold

**Note:** For ease of communications, Teams channels support access for Guests directly and Federated Guest. This allows other Office 365 tenant organizations to be granted access and connected via domain name or IP address.

Teams supports integration from from many apps and outside sources, such as KRONOS and Bots. This opens the door for integration of other programs and applications to be shared with patients and healthcare teams by pulling patient data from several Electronic Health Record (EHR) vendors using FHIR within the continuity of care continuum.[9] Steps need to be taken to control access, logging, exposure of that ePHI data while having "break the glass". Break the glass (or break-glass) allows caregivers access to information without the need to extend existing permissions. Access is provided to information needed but normally not accessible as part of day-to-day need-to-know. The system should document (audit) any actual access for later review. Office 365 Information Protection Tools give compliance personnel the tools needed to achieve this level of control. Details and guidance are discussed in **Part 3: Microsoft Office 365, Teams and HIPAA Traceability Section**.

## Office 365 Security & Compliance Center

By leveraging Office 365 E5 business subuscription, organizations have access to a host of other tools including Office 365 Information Protection tools to manage Office 365, Teams and other core Microsoft services.

Access to these additional roles can be assigned to regular User Accounts (read: Domain Administrator-level access is NOT REQUIRED) to perform tasks in the Office 365 Security & Compliance Center. The role groups available at the time of this whitepaper include the following:

1. **Compliance Administrator**
   Manages settings for device management, data protection, data loss prevention, reports, and preservation.

2. **Security Operator**
   Manages security alerts, and also view reports and settings of security features.

3. **Reviewer**
   Members of this management role group have permissions to manage and dispose record content.

4. **Records Management**
   Members of this management role group have permissions to manage and dispose record content.

5. **Organization Management**
   Members of this management role group have permissions to manage Exchange objects and their properties in the Exchange organization. Members can also delegate role groups and management roles in the organization. This role group shouldn't be deleted.

6. **Compliance Administrator**
   Manages settings for device management, data loss prevention, reports, and preservation.

7. **Supervisory Review**
   Control policies and permissions for reviewing employee communications.

[9] https://techcommunity.microsoft.com/t5/Microsoft-Teams-Blog/Integrate-electronic-health-records-into-Microsoft-Teams-care/ba-p/334042

### 8 Security Administrator

Smaller subset of assigned-roles than **Compliance Administrator:** Manages settings and policies for data retention, loss, audit logs and device management.

### 9 Security Reader

View-only access to alerts, device management, DLP and security logs.

### 10 eDiscovery Manager

Perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations.

### 11 Service Assurance User

Access the Service Assurance section in the Office 365 Security & Compliance Center. Members of this role group can use this section to review documents related to security, privacy, and compliance in Office 365 to perform risk and assurance reviews for their own organization.

### 12 MailFlow Administrator

Views recipients.  Use Exchange Admin Center to set permissions.

### 13 Data Investigator

Perform searches on mailboxes, SharePoint Online sites, and OneDrive for Business locations.

The mission of Office 365 Security & Compliance Center is to be a one-stop portal for protecting all data in Office 365 and the above roles should be granted to Compliance, Security and Executives in the organization.

For additional Microsoft resources including granting access to data security and compliance teams in your Office 365 and Teams organization, view the following resources:

- **Manage your organization's Security and Compliance Administrative panel for Microsoft Office 365 and Teams**
  https://protection.office.com
- **Give users access to the Office 365 Security & Compliance Center**
  https://docs.microsoft.com/en-us/office365/securitycompliance/grant-access-to-the-security-and-compliance-center
- **About Office 365 admin roles**
  https://docs.microsoft.com/en-us/office365/admin/add-users/about-admin-roles?redirectSourcePath=%252farticle%252fda585eea-f576-4f55-a1e0-87090b6aaa9d&view=o365-worldwide

The following section reviews HIPAA Security regulations as selected by the OCR HIPAA Audit Protocol and provides guidance where customer's responsibilities lie with Office 365 and Teams to meet HIPAA compliance and provide a solid foundation in data security controls.

## Part 3

# MICROSOFT OFFICE 365, TEAMS AND HIPAA TRACEABILITY SECTION

With an explosive growth of cloud-usage and corresponding data communications, we at HIPAA One have done extensive research on how to configure Office 365 and Teams to meet HIPAA and other mandates and certifications requiring NIST-based controls. Preparing for HIPAA enforcement audits starts with due diligence for business associates – such as Microsoft Office 365 with Teams implementation. Microsoft has undergone its own HIPAA Security and Privacy compliance assessment following their responsibilities as a business associate[10]. In addition, Microsoft will provide Business Associate Agreements (BAA) for any Microsoft SharePoint-enabled customer dealing with ePHI via the Microsoft Trust Center[11].

The following table provides insight regarding customers compliance with the HIPAA Audit Protocol[12] using Office 365 and Teams while building a strong foundation of modern security controls. Failure to apply some recommended and documented hardening strategies for Office 365 and Teams in a healthcare environment may expose organizations to potential HIPAA violations and potential penalties aforementioned in Part 1.

Meeting security, privacy, and compliance requirements is a shared responsibility between the customer and Microsoft as the cloud service provider[13]. The compliance section below indicates Y or N when Office 365 and Teams can be configured under the customer's managed responsibilities to enforce controls defined by the organization's HIPAA Security Policies and Procedures.

Office 365 and Teams Compliant Values are as follows:

**"Y" :** Customer may implement control with provided feature to achieve compliance with the HIPAA section.

**"N" :** Option not available for the customer to implement the security control therefore may not be compliant with the HIPAA section.

**"-" :** Must be performed separately or outside of the Office 365 and Teams cloud application environment.

[10] Azure – HIPAA Security and Privacy Assessment Report 2017, Coalfire, Shannon Wittemore, Sharon Laivand July 25, 2017.

[11] HIPAA Business Associate Agreement, February 2018, Microsoft Corporation. Also found here: https://www.microsoft.com/en-us/TrustCenter/Compliance/HIPAA

[12] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html HIPAA Audit Protocol, Office for Civil Rights, August 17, 2018

[13] https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

## Customer-Managed HIPAA Controls for Microsoft Office 365 and Teams

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| administrative | §164.308(a) | Security Management Process | P&P to manage security violations | - | Microsoft Office 365 has an abundance of security controls outlined in this whitepaper to enable procedures in this over-arching policy statement for technical and some administrative controls. | - | Microsoft Teams is a unified communications platform that combines persistent workplace chat, video meetings, file storage, and application integration. Teams is integrated with the company's Office 365 Information Protection Tools and Security and Compliance Center. |
| administrative | §164.308(a)(1)(ii)(A) | Security Management Process -- Risk Analysis | Conduct vulnerability assessment | - | HIPAA Security Risk Analysis is the cornerstone of any compliance initiative and should be updated annually to keep current with emerging threats in healthcare.  This effort may be conducted using HIPAA One[14]. | - | Same as Office 365. |
| administrative | §164.308(a)(1)(ii)(B) | Security Management Process -- Risk Management | Implement security measures to reduce risk of security breaches | Y | Evolving security threats can have Office 365 controls implemented to maintain confidentiality, integrity and availability of ePHI while addressing Technical, Administrative and Physical Safeguards. See below for Office 365 controls available which are mapped to HIPAA Citations below to be managed by the customer. | - | Controlled in Office 365. |
| administrative | §164.308(a)(1)(ii)(C) | Security Management Process – Sanction Policy | Workforce sanction for P&P violations | Y | Sharing user IDs, phishing, browsing ePHI or sending ePHI to the wrong party and other violations of this policy can be detected, mitigated and policy statement implemented using Skype for Business User Policies, Multi-Factor Authentication (MFA), Advanced Threat Protection Safe Links (ATP) E5, data classification & loss prevention and audit logging from Security and Compliance Package E3. | - | Controlled in Office 365. |

[14] www.hipaaone.com/contact-us

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| administrative | §164.308(a)(1)(ii)(D) | Security Management Process --Information System Activity Review | Procedures to review system activity | Y | 3 sets of logs to collect: Azure login logs, Azure sign-in logs (located in Azure Active Directory), and audit logs located in the Security & Compliance Center.<br>Microsoft Secure Score for CIOs only works for those with E5 licensing.<br>Review Office 365 Security and Compliance Reports -> Dashboards for suspicious activity.<br>Configure Office 365 Security and Compliance Reports -> Alert Policies to track user and admins activities, malware threats or data loss incidents and alert when they are detected.<br>Setup Advanced Threat Protection analytics to detect patterns of access. ATP leverages Artificial Intelligence to develop learning models looking at behavior and characteristics. | Y | Teams admin center -> Analytics & Reports shows last 7 or 28 days of user activity.<br>Controlled in Office 365. |
| administrative | §164.308(a)(2) | Assigned Security Responsibility | Identify security official responsible for P&P | Y | Microsoft 365 admin center -> Settings -> Security & Privacy -> Privacy profile -> set privacy contact.<br>E5 and enabling Security and Compliance Roles will grant security official access to fulfill their responsibilities. | Y | Controlled in Office 365. |
| administrative | §164.308(a)(3)(i) | Workforce Security | Implement P&P to ensure appropriate ePHI access | Y | Multi-factored authentication (MFA) Home -> Active Users -> User -> Manage Multi-Factored Authentication will ensure compromised accounts do not have unauthorized access. and Privileged access management in Microsoft Office 365 based on user permissions. | - | Guest access may be turned on to access Teams however, ensure guests are authorized and push the same Security & Compliance policies (i.e. MFA, DLP, etc.) applied to their accounts as configured in Office 365.[15] |

[15] https://docs.microsoft.com/en-us/microsoftteams/guest-access

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| | | | | | Data Loss Prevention Polices must be set & verified.<br>Data Classification Labels can detect & label ePHI. The customer must secure folder-level permissions and manage group membership. | | Set DLP policies to include Teams external user from access: Applying DLP Policies to Teams is in the process of being released by Microsoft and may be available post-publication of this whitepaper[16]. |
| administrative | §164.308(a)(3)(ii)(A) | Workforce security -- Authorization and/or Supervision | Authorization supervision for ePHI access | Y | Advance Threat Protection (ATP), Log Analytics workspace, Data classification, break glass and privileged access. | Y | Dashboard -> Manage Teams to manage users and channels that may contain ePHI. |
| administrative | §164.308(a)(3)(ii)(B) | Workforce security -- Workforce Clearance Procedure | Procedures to ensure appropriate ePHI access | Y | Ensure Domain Admin receives notice from HR and applies user security groups and policies according to their requested level of access.<br>Can use authorization by domain admin before new domain admins can be added. After identifying where ePHI is using Data Classification, setup groups who have access to these folders containing ePHI. | Y | User must have an Office 365 Account and Teams app enabled before access can be granted. |
| administrative | §164.308(a)(3)(ii)(C) | Workforce security -- Establish Termination Procedures | Procedures to terminate ePHI access | Y | Account termination for Office 365 and account assignment for One Drive and Email. Admin Center-> Users -> Active Users -> Block Sign-in or Delete. | Y | If users are terminated or disabled, Teams access is also disabled. |
| administrative | §164.308(a)(4)(i) | Information Access Management | P&P to grant access to ePHI | Y | Admin Center -> Groups -> Security Group (or Office 365 Group). Then add group permissions to SharePoint folders and users to those group. Can enter in user description, name, position, location, type, dates of access with expiration, type of equipment used for access, multi-factor authentication in the User or Group properties established above. | Y | User must have an Office 365 Account and Teams app enabled before access can be granted. |

[16] https://techcommunity.microsoft.com/t5/Microsoft-Teams-Blog/What-s-new-in-Microsoft-Teams-the-Enterprise-Connect-feature/ba-p/376255

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| administrative | §164.308(a)(4)(ii)(A) | Information Access Management -- Isolating Healthcare Clearinghouse Functions | P&P to separate ePHI from other operations | Y | Can separate data by folders, roles and security groups in Office 365. See above §164.308(a)(4)(i). Managed. | - | This is performed outside of the application. |
| administrative | §164.308(a)(4)(ii)(B) | Information Access Management -- Access Authorization | P&P to authorize access to ePHI | - | Separate forms and contracts are performed outside of the application. | - | Separate forms and contracts are performed outside of the application. |
| administrative | §164.308(a)(4)(ii)(C) | Information Access Management -- Access Establishment and Modification | P&P to grant access to ePHI | Y | Changes in access to ePHI can be enabled using Admin Center -> Groups -> Security Group (or Office 365 Group). Then add group permissions to SharePoint folders and users to those group. Can enter in user description, name, position, location, type, dates of access with expiration, type of equipment used for access, multi-factor authentication in the User or Group properties established above. | - | This is performed outside of the application. |
| administrative | §164.308(a)(5)(i) | Security Awareness and Training | Training program for workforce | - | This is performed outside of the application.<br>Cybersecurity, HIPAA and simulated email phishing campaigns may be provided by HIPAA One. | - | This is performed outside of the application. |
| administrative | §164.308(a)(5)(ii)(A) | Security Awareness and Training -- Security Reminders | Distribute periodic security updates | N | Use standard Outlook emails, or Teams & update Login announcements. | - | This is performed outside of the application. |

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| administrative | §164.308(a)(5)(ii)(B) | Security Awareness, Training, and Tools -- Protection from Malicious Software | Procedures to guard against malicious software | Y | Security & Compliance Center -> Threat Management -> Policy -> ATP Safe Attachments -> Turn on ATP for SharePoint, OneDrive, and Microsoft Teams. Create a Policy and configure appropriate settings if an attachment is malicious. | Y | Controlled in Office 365.<br>Controlling side-loading of BOTs and apps from being installed: Teams supports integration from many apps by default such as KRONOS and Bots[17] need to be controlled individually. To control go to: Admin Center -> Settings -> Services & add-ins -> Microsoft Teams -> Apps -> allow external apps (check box next to each approved app) then turn off uploading of external apps.[18] |
| administrative | §164.308(a)(5)(ii)(C) | Security Awareness, Training, and Tools -- Log-in Monitoring | Procedures and monitoring of log-in attempts | Y | Security & Compliance Center -> Alerts -> Manage Advanced alerts -> Go to Office 365 Cloud App Security (may need to turn on first) -> Control -> Policies -> Multiple Failed Login Attempts | Y | Controlled in Office 365. |
| administrative | §164.308(a)(5)(ii)(D) | Security Awareness, Training, and Tools -- Password Management | Procedures for password management | Y | Microsoft 365 admin center -> Settings -> Security & Privacy -> Password policy. | Y | Controlled in Office 365. |
| administrative | §164.308(a)(6)(i) | Security Incident Procedures | Policies and procedures to manage security incidents | Y | Security & Compliance Center -> Alert Policies -> configure to notify the security official of potential security incidents for appropriate management. | Y | Per notes in Office 365., set the alert policies for External user file activity, DLP policy match, and others as appropriate for Teams. |
| administrative | §164.308(a)(6)(ii) | Security Incident Procedures -- Response and Reporting | Mitigate and document security incidents | - | Separate forms and contracts are performed outside of the application. | - | Separate forms and contracts are performed outside of the application. |
| administrative | §164.308(a)(7)(i) | Contingency Plan | Emergency response P&P | - | Separate forms and contracts are performed outside of the application. | - | Separate forms and contracts are performed outside of the application. |

[17] https://docs.microsoft.com/en-us/azure/bot-service/bot-service-channel-connect-email?view=azure-bot-service-4.0

[18] https://docs.microsoft.com/en-us/microsoftteams/admin-settings

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| administrative | §164.308(a)(7)(ii)(A) | Contingency Plan – Data Backup Plan | Data backup planning & procedures | Y | OneDrive and SharePoint can restore deleted files based on retention policy. Site collections can be restored and configured. Alternatively, manually backups may also be performed. | Y | Controlled in Office 365. |
| administrative | §164.308(a)(7)(ii)(B) | Contingency Plan –Disaster Recovery Plan | Data recovery planning & procedures | Y | Office 365 uses multiple geo-based data centers. Storage data replicated multiple times. Fabric is designed to be backed up and restored from checkpoints. | Y | Controlled in Office 365. |
| administrative | §164.308(a)(7)(ii)(C) | Contingency Plan -- Emergency Mode Operation Plan | Business continuity procedures | Y | Office 365 uses multiple geo-based data centers. Storage data replicated multiple times. Fabric is designed to be backed up and restored from checkpoints | Y | Controlled in Office 365. |
| administrative | §164.308(a)(7)(ii)(D) | Contingency Plan -- Testing and Revision Procedure | Contingency planning periodic testing procedures | Y | Office 365 uses multiple geo-based data centers. Storage data replicated multiple times. Fabric is designed to be backed up and restored from checkpoints | Y | Controlled in Office 365. |
| administrative | §164.308(a)(7)(ii)(E) | Contingency Plan --Application and Data Criticality Analysis | Prioritize data and system criticality for contingency planning | Y | Office 365 uses multiple geo-based data centers. Storage data replicated multiple times. Fabric is designed to be backed up and restored from checkpoints. | Y | Controlled in Office 365. |
| administrative | §164.308(a) (8) | Evaluation | Periodic security evaluation | - | Microsoft Secure Score is designed to be constantly evaluating the configuration of customer Office 365 tenant. This provides recommendations to the Covered Entity to apply configuration changes. The evaluation happens at least once a day. Compliance Manager may be used to perform periodic technical and non-technical evaluations. | - | Controlled in Office 365. |

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| administrative | §164.308(b)(1) | Business Associate Contracts and Other Arrangements | Obtain satisfactory assurances | Y | Office 365 provides HIPAA & HITECT assurances, BAA can be obtained online. | Y | Controlled in Office 365. |
| administrative | §164.308(b)(3) | Business Associate Contracts and Other Arrangements -- Written Contract or Other Arrangement | Obtain satisfactory assurances | Y | Office 365 provides HIPAA & HITECH assurances, BAA can be obtained online. | Y | Controlled in Office 365. |
| physical | §164.310(a)(1) | Facility Access Controls | Physical safeguards for authorized server access | - | This is performed outside of the application. | - | This is performed outside of the application. |
| physical | §164.310(a)(2)(i) | Facility Access Controls -- Contingency Operations | Procedures to support emergency operations and recovery | - | This is performed outside of the application. | - | This is performed outside of the application. |
| physical | §164.310(a)(2)(ii) | Facility Access Controls -- Facility Security Plan | P&P to safeguard equipment and facilities | - | This is performed outside of the application. | - | This is performed outside of the application. |
| physical | §164.310(a)(2)(iii) | Facility Access Controls -- Access Control and Validation Procedures | Facility access procedures for personnel | - | This is performed outside of the application. | - | This is performed outside of the application. |

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| physical | §164.310(a)(2)(iv) | Facility Access Controls -- Maintain Maintenance Records | P&P to document security-related repairs and modifications | - | This is performed outside of the application. | - | This is performed outside of the application. |
| physical | §164.310(b) | Workstation Use | P&P to specify workstation environment & use | - | This is performed outside of the application. | - | This is performed outside of the application. |
| physical | §164.310(c) | Workstation Security | Physical safeguards for workstation access | - | This is performed outside of the application. | - | This is performed outside of the application. |
| physical | §164.310(d)(1) | Device and Media Controls | Document hardware and media movement | - | This is performed outside of the application. | - | This is performed outside of the application. |
| physical | §164.310(d)(2)(i) | Device and Media Controls -- Disposal | P&P to manage media and equipment disposal | - | Failed disks used within Office 365 datacenters are physically destroyed and audited through the ISO process. | - | This is performed outside of the application. |
| physical | §164.310(d)(2)(ii) | Device and Media Controls -- Media Re-use | P&P to remove ePHI from media and equipment | - | This is performed outside of the application. | - | This is performed outside of the application. |
| physical | §164.310(d)(2)(iii) | Device and Media Controls -- Accountability | Document hardware and media movement | - | This is performed outside of the application. | - | This is performed outside of the application. |

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| physical | §164.310(d)(2)(iv) | Device and Media Controls -- Data Backup and Storage Procedures | Backup ePHI before moving equipment | - | This is performed outside of the application. | - | This is performed outside of the application. |
| technical | §164.312(a)(1) | Access Control | P&P to grant access to ePHI | - | This is performed outside of the application. | - | This is performed outside of the application. |
| technical | §164.312(a)(2)(i) | Access Control -- Unique User Identification | Assign unique IDs to support tracking | Y | Office 365 user ID uses unique email address base on business domain name. | Y | Other Office 365 tenants are by default federated and may be added to Teams without compromising unique user identification. Controlled in Office 365.[19] |
| technical | §164.312(a)(2)(ii) | Access Control -- Emergency Access Procedure | Procedures to support emergency access | Y | To enable "break the glass" access, use Data Loss Prevention -> Create (or edit) Policy -> set content for sensitive info Policy Settings -> User overrides "Let people who see the tip override the policy and share the content" is ON -> Require a business justification to override is ON.<br>Domain Admin Emergency access available provided.[20] | N | Controlled in Office 365.<br>Set "break the glass" DLP policies to include Teams external user from access: Applying DLP Policies to Teams is in the process of being released by Microsoft and may be available post-publication of this whitepaper[21]. |
| technical | §164.312(a)(2)(iii) | Access Control -- Automatic Logoff | Session termination mechanisms | Y | Idle Session threshold for SharePoint & OneDrive can be configured manually using SharePoint Online Management Shell.[22] | Y | Controlled in Office 365. |
| technical | §164.312(a)(2)(iv) | Access Control -- Encryption and Decryption | Mechanism for encryption of stored ePHI | Y | Data at rest (Bitlocker) and data in transit (TLS) used for encryption.[23] | Y | Controlled in Office 365. |

[19] https://docs.microsoft.com/en-us/microsoftteams/let-your-teams-users-communicate-with-other-people

[20] https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access

[21] https://techcommunity.microsoft.com/t5/Microsoft-Teams-Blog/What-s-new-in-Microsoft-Teams-the-Enterprise-Connect-feature/ba-p/376255

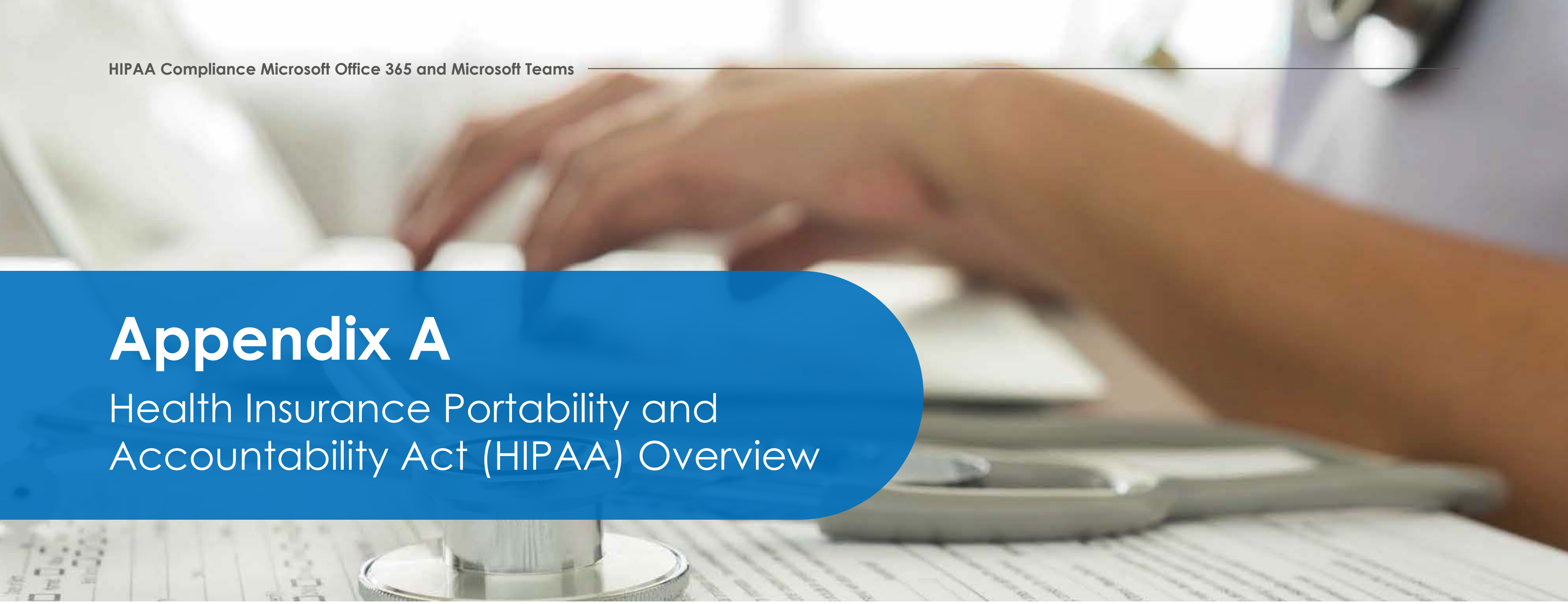
[22] https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Idle-Session-Timeout-Policy-in-SharePoint-Online-amp-OneDrive-is/ba-p/211274

[23] https://docs.microsoft.com/en-us/office365/securitycompliance/encryption

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| technical | §164.312(b) | Audit Controls | Procedures and mechanisms for monitoring system activity | Y | Security & Compliance Center -> Alerts -> Manage Advanced alerts -> Go to Office 365 Cloud App Security (may need to turn on first) -> Control -> Policies -> <set as needed>. | Y | In the Office 365 Security & Compliance Center, choose Reports > Dashboard > Threat Protection Status -> View details table. |
| technical | §164.312(c)(1) | Integrity | Policies and procedures to protect ePHI from improper alteration or destruction | Y | Threat management, security monitoring, and file/data integrity prevent or detect any tampering of data. | Y | Controlled in Office 365. |
| technical | §164.312(c)(2) | Integrity -- Mechanism to Authenticate ePHI | Mechanisms to corroborate ePHI not altered | Y | Using Office 365 forces only authorized users with Multi-Factored Authentication (enabled) avoids improper or accidental destruction or alteration of ePHI. | Y | Controlled in Office 365. |
| technical | §164.312(d) | Person or Entity Authentication | Verify identity of those seeking access to ePHI | Y | Do not share user IDs.  Active Directory enforces unique user identification, and ensures unique user, device, role and group identifiers are never reused. | Y | Controlled in Office 365. |
| technical | §164.312(e)(1) | Transmission Security | Measures to ensure integrity of ePHI on transmission | Y | Office 365 provides FIPS 140-2 validated cipher support for customer connections, interconnected system connections, and remote access connections to Office 365. | Y | Controlled in Office 365. |
| technical | §164.312(e)(2)(i) | Transmission Security -- Integrity Controls | Measures to ensure ePHI is not improperly modified without detection until disposed of | Y | Force encryption for ePHI: Security & Compliance Center -> Data loss prevention -> Policy to encrypt email messages when content matches HIPAA Insurance Act template.<br>Office 365 provides FIPS 140-2 validated cipher support for customer connections, interconnected system connections, and remote access connections to Office 365. | Y | Controlled in Office 365. |

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| technical | §164.312(e)(2)(ii) | Transmission Security --Encryption | Mechanism for encryption of transmitted ePHI | Y | Force encryption for ePHI: Security & Compliance Center -> Data loss prevention -> Policy to encrypt email messages when content matches HIPAA Insurance Act template.<br>Office 365 provides FIPS 140-2 validated cipher support for customer connections, interconnected system connections, and remote access connections to Office 365. | Y | Controlled in Office 365. |
| organizational | 164.314(a)(1) | Business Associate Contracts or Other Arrangements | Approval process for contract template deviations | - | This is performed outside of the application.<br>HIPAA One offers 3rd-party BAA management solution to address this requirement. | - | This is performed outside of the application. |
| organizational | 164.314(a)(2)(i) | Business associate contracts | BAAs must state the Business Associate must comply with HIPAA | - | This is performed outside of the application.<br>HIPAA One offers 3rd-party BAA management solution to address this requirement. | - | This is performed outside of the application. |
| organizational | §164.316(a) | Policies and Procedures | Implement P&P and actions & activities | - | This is performed outside of the application. | - | This is performed outside of the application. |
| organizational | §164.316(b)(1) | Documentation | Document P&P and actions & activities | - | This is performed outside of the application. | - | This is performed outside of the application. |

| Section | Citation | Key Activity | Description | Office 365 Compliant? Y/N | Notes | Teams Compliant? Y/N | Notes |
|---|---|---|---|---|---|---|---|
| organizational | §164.316(b)(2) (i) | Documentation – Time Limit | Retain documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later | Y | 6-year retention can be defined through Office 365 Security & Compliance Center. Mailboxes must have archive mailboxes enabled, retention tags for the archive and deletion policies must be created, retention policy created, and retention tags added, and assignment of the retention policy to user & group mailboxes - noting retention policy may also be set as the default for the covered entity. | Y | Global retention is allowed based on the number of years however, Data Governance -> Advanced Retention for Teams is not available in the current version at time of publishing this whitepaper. |
| organizational | §164.316(b)(2) (ii) | Documentation-Availability | Documentation available to system administrators | Y | Logs and reports of system activity to monitor threats to ePHI is available through Security & Compliance Center Roles for security and compliance personnel.<br>Retention of default logs needs to be extended through PowerShell. | - | Controlled in Office 365. |
| organizational | §164.316(b)(2) (iii) | Documentation – Updates | Periodic review and updates to changing needs | Y | Post-implementation of Office 365 security controls need to be reviewed and updated with new features and/or implementing granular controls to stay relevant in the "block and tackle" of detecting, mitigating and managing security incidents. This is a combination of an Organization and Microsoft's ongoing commitment to manage emerging threats to healthcare organizations. | Y | Controlled in Office 365. |



# Appendix A

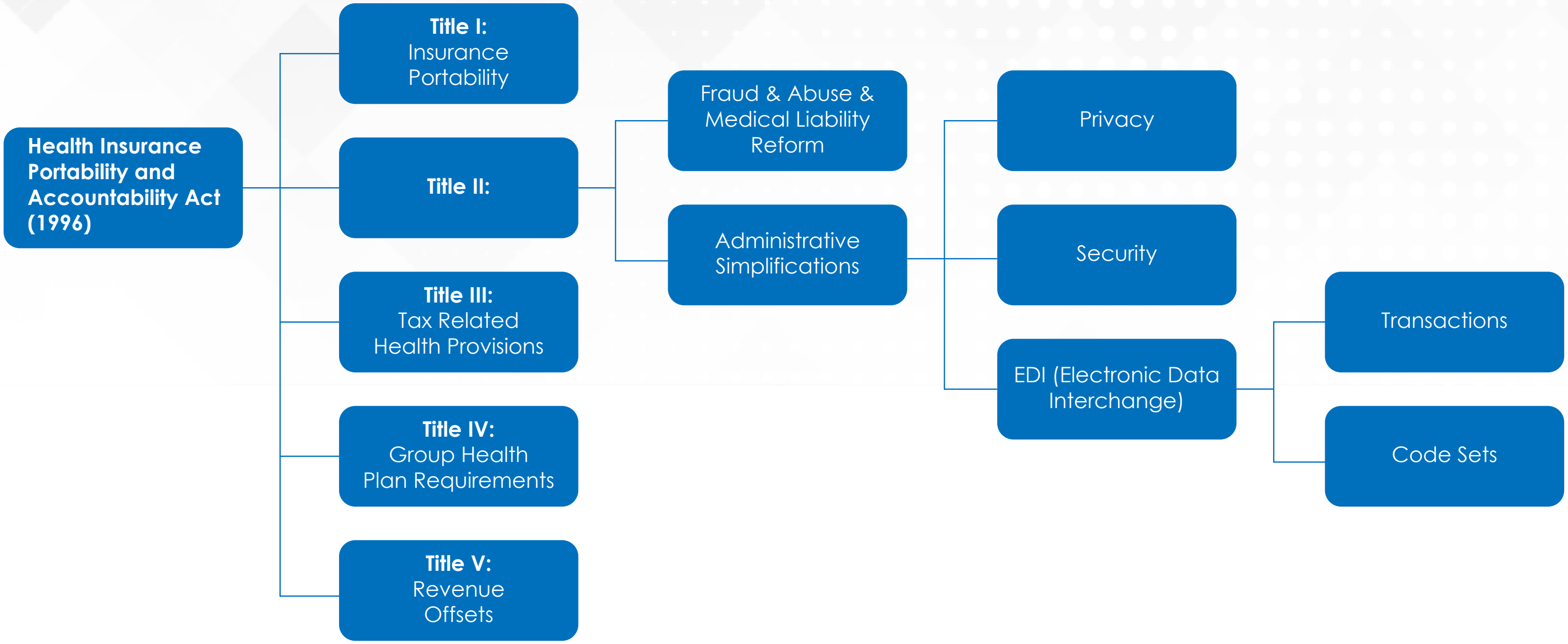
## Health Insurance Portability and Accountability Act (HIPAA) Overview

The Health Insurance Portability and Accountability Act was passed and signed into law on August 21, 1996, adding a new part C to title XI of the Social Security Act (sections 1171–1179.)  Its inception was triggered by a growing awareness that American citizens were not provided basic rights to their own health information; specifically, the right to protect their personal information and retain a copy of their own health records. Throughout the 1980's and 1990's, the federal government began receiving complaints stating they were not prepared to handle the mounting issue.

Early on, clinics and hospitals were not open to sharing medical records with patients for a number of reasons, including fear of competition and lack of internal processes to handle patient record requests.

Healthcare was late to embrace technology for patient care compared to most other industries. In the mid 2000's, splashy headlines read that America's healthcare costs were amounting to more of its Gross Domestic Product (GDP) than any other developed nation, and higher than the entire GDP of many third-world countries.  The trend of increasing health insurance premiums over-shadowed the increase in medical care costs as both those who could pay and those who could not were burdened.

In 2009, as the world experienced a global recession, a still paper-based healthcare industry was experiencing skyrocketing costs. Pursuant to the American Recovery and Reinvestment Act (ARRA) passed by President Obama in 2009, $29 billion was earmarked under the HITECH Act to


Health Insurance Portability and Accountability Act (1996)
Title I: Insurance Portability
Title II:
Title III: Tax Related Health Provisions
Title IV: Group Health Plan Requirements
Title V: Revenue Offsets
Fraud & Abuse & Medical Liability Reform
Administrative Simplifications
Privacy
Security
EDI (Electronic Data Interchange)
Transactions
Code Sets

provide incentives to Covered Entities (hospitals and clinic-based doctors). And with that, Meaningful Use was born.

While these changes were taking place, proactive enforcement of HIPAA's basic privacy and security standards were sorely lacking.  Millions of records storing personal identities within big-data demographics were being converted to electronic personal health records without ensuring the security of the data. Across the healthcare landscape, medical records were unsecured and exposed. As a result, patient health data began being lost, stolen or inappropriately viewed/disclosed.

That same year, the Office for Civil Rights (OCR) was commissioned with the authority to enforce the HIPAA Security and Breach Notification Rules. This authority allowed the OCR to develop an audit standard, strategy and process to respond to patient complaints and enforce the standards.

As required by the Health Information Technology for Economic and Clinical Health Act (HITECH) (February 17, 2009), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) and HIPAA's final "HIPAA Omnibus rule" (January 25, 2013); OCR issued a final "Guidance on Risk Analysis Requirements under the HIPAA Security Rule" on July 14, 2010. The guidance incorporated

NIST-based risk methodologies for entities to use when conducting a HIPAA Security Risk Analysis.

The HITECH Act granted OCR the authority to enforce all of the requirements of the HIPAA Security Rule and limited requirements of the HIPAA Privacy Rule directly against "business associates" of "covered entities."[24] Covered entities include hospitals, medical billing centers, health insurance companies, healthcare clearinghouses and other healthcare providers. The HITECH Act also expanded HIPAA's already broad "business associates" definition, which includes: health information exchange organizations, e-gateways handling ePHI and subcontractors that create, receive, maintain, or transmit PHI on behalf of a business associate[23].

Increased enforcement to ensure covered entities and business associates are compliant with the HIPAA Security, Privacy and Breach Notification Rules has raised public awareness for the need to protect PHI. In recent years, the OCR has taken significant strides by obtaining monetary payments through settlements with providers who have failed to take reasonable and appropriate safeguards to protect their ePHI.

Under the HITECH Act and HIPAA's Omnibus rule, covered entities and business associates must also comply with rigorous breach notification rules when PHI is compromised. For example, if the number of patients affected by a data privacy breach is more than 500 in a given state or jurisdiction, the media must be notified.[26]

PHI is individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to any of the following:

1. The past, present or future physical or mental health or condition of an individual
2. Provision of healthcare to an individual
3. Payment for the provision of healthcare to an individual

[24] HITECH Act Subtitle D, Section 13401.
[25] HITECH Act Subtitle D, Section 13408.
[26] HITECH Act Subtitle D, Section 13402.
[27] 45 CFR § 164.312(b).

If the information identifies or provides a reasonable basis to identify an individual, it is considered individually identifiable health information. Elements that make health information individually identifiable include, but are not limited to, the following 18 Identifiers:

1. Names
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
    1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and
    2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section[28].

[28] 45 C.F.R. § 164.514(b).

**The HIPAA Security Rule imposes standards in five categories:** administrative safeguards, physical safeguards, technical safeguards, organizational requirements, and documentation requirements (policies, procedures, etc.).

The HIPAA Security Rule contains standards, which must be implemented and implementation specifications, which are designated as either "required" or "addressable." Entities must implement those specifications designated as "required." For specifications designated as "addressable" entities must assess whether the particular specification is reasonable and appropriate based on its environment and, if it is not, entities must document why it is not reasonable and appropriate and implement an alternative measure.

**Required:** If an implementation specification is marked as "required," it must be implemented by every covered entity.

While the databases of Electronic Health Record (EHR) systems are obvious areas where ePHI resides, there are many other systems in which ePHI may be stored or transmitted, including personal (implanted) medical devices, modern medical equipment, tablets, cell phones, copiers, scanners, fax machines, multi-function devices, print servers, ePHI databases, encrypted email, voice mail servers, security camera systems, protected file servers, network shared drives and even on local machines.

These "adjunct" areas of ePHI storage may or may not be within the organization's policy restrictions. Compliance with protecting all ePHI, however, is required. A table reflecting the current penalty amounts for violations of HIPAA[29] follows:

Table 2
Categories of Violations and Respective Penalty Amounts Available

Updated annually per adjustments published in the Federal Register pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015."

| Violation category - Section 1176(a)(1) | Each violation | All such violations of an identical provision in a calendar year |
|---|---|---|
| (A) Did Not Know | $114 - $57,051 | $1,711,533 |
| (B) Reasonable Couse | $1,141 - $57,051 | $1,711,533 |
| (C) (i) Willful Neglect - Corrected | $11,410 - $57,051 | $1,711,533 |
| (D) (II) Willfull Neglect - Not Corrected | $57,051 | $1,711,533 |

The HIPAA Privacy Rule addresses PHI in any medium, while the HIPAA Security Rule applies to PHI in electronic form. Covered Entities are bound by both Rules while Business Associates must comply with all of the provisions of the HIPAA Security Rule and some provisions of the HIPAA Privacy Rule.

[29] See page 5583 of the Federal Register, January 25, 2013. Reference "TABLE 2—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE"

# Appendix B

## General Data Protection Regulation (GDPR) Overview

As a starting point, any person or company seeking to process the personal data of another individual must:

1. Clearly disclose any data collection and use;
2. Declare the lawful basis and purpose for data processing; and
3. State how long data is being retained and whether it is being shared with any third parties or outside of the EEA.

GDPR defines "processing" as follows: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "(Article 4, Definitions)

## Article 5 - Principles Relating to the Processing of Personal Data

The manner, purpose, and scope of the data processing are key issues relating to GDPR. Article 5 states that, with regards to processing personal data, it shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject; ('lawfulness, fairness and transparency');
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes('purpose limitation');
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')

## Article 6 - Lawfulness of Processing

Processing shall be lawful only if and to the extent that at least one of the following applies:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller is subject;
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

## Article 7 - Conditions for Consent

For consent to be valid under the GDPR it must meet certain requirements such as: (1) the consent must be freely given; (2) the consent must be "clearly distinguishable from other matters" if it is written; (3) the consent must be in an "intelligible and easily accessible form;" and (4) must use clear and plain language. The data subject may withdraw consent at any time and it "shall be as easy to withdraw as to give consent." Data subjects, therefore, have the right to opt in and opt out in a non-burdensome manner and data processors must respond accordingly. (Article 7)

## Articles 12-23 - Rights of the Data Subject

— GDPR gives data subjects more control and rights regarding their personal data. For example, the GDPR grants data subjects the right to be informed, of access, to rectification, to easure, to restrict processing, to data portability, to object, and rights regarding automated decision making including profiling.

## Articles 31 & 32

— Data breach notifications play a large role in the GDPR text. Article 31 specifies requirements for single data breaches: controllers must notify Supervisory Authorities of a personal data breach within 72 hours of learning of the breach and must provide specific details of the breach such as the nature of it and the approximate number of data subjects affected. Article 32 requires data controllers to notify data subjects as quickly as possible of breaches when the breaches place their rights and freedoms at high risk.

## Articles 35 - Data Protection Impact Assessment

— Due to the extensive nature of the GDPR and the potential risks that exist for anyone processing personal data, there are situations which require a Data Protection Impact Assessment (DPIA) when the type of processing "is likely to result in a high risk to the rights and freedoms of natural persons." Article 35. Specifically, an assessment is required when:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- Processing on a large scale of special categories of data or of personal data relating to criminal convictions and other offenses;
- A systematic monitoring of a publicly accessible area on a large scale.

## Articles 37

— Article 37 outlines the data protection officer position and its responsibilities in ensuring GDPR compliance as well as reporting to Supervisory Authorities and data subjects.

## Articles 44-50 - Transfers of Personal Data to Third Countries or International Organizations

— The GDPR outlines principles, requirements and different mechanisms for cross-border transfers of personal data outside of the EU/EEA.

## Articles 77-84 - Remedies, Liability and Penalties

— The GDPR outlines the complaint process for a data subject to lodge a complaint with a Supervisory Authority (SA). It also describes the remedies, liabilities and potential liabilities and penalties for violations under the GDPR.

As GDPR applies to a major portion of the developed world and countries that do business there, its regulations and implications reach far and wide. It is vital that businesses and individuals do their due diligence to maintain strict compliance with GDPR's regulations.