HIPAA Compliance with Microsoft 365

Microsoft

Intraprise HEALTH + HIPAA One

intraprisehealth.com

801-770-1199

Contributors

Brian Parks
SVP Information Security Services
Intraprise Health

Neal Pason
Chief Operating Officer
Intraprise Health

Bobby Seegmiller
Executive VP
Intraprise Health

Dallin Southwick
Security Consultant
Intraprise Health

Alan Davis, GSLC
Principal
Proteus Consulting

Jon Sparks, CISSP
Engineering Manager
WingSwept

Why This Update?

In the two years since publishing their original Microsoft-supported whitepaper, HIPAA One has been integrated into the Intraprise Health family while Microsoft has continued maturing new cloud-based information services. In a collaborative effort, Intraprise Health reached out to Proteus Consulting, who partnered with WingSwept to document the changes and proposals that the U.S. Department of Health and Human Services (HHS) published in response to COVID-19, and to describe the importance of information security in the Microsoft 365 services platform.

Proteus Consulting of Hayden, Idaho works with their partner-clients on managing risk, compliance, and information security. WingSwept of Garner, North Carolina is a premier managed services provider in the small and medium business market.

Intraprise Health is a full-service cybersecurity firm. Their software offerings include: HIPAA One®, NIST Framework Assessment, and BluePrint Protect Risk Management software. Their services include HITRUST Assessments, security risk assessment and remediation services.

Contents

ABSTRACT

This document provides healthcare executives, management, and administrative teams the necessary information to assess HIPAA compliance and cybersecurity diligence using Microsoft 365. By addressing the controls found in this whitepaper, healthcare organizations may significantly reduce the likelihood of breaches while working towards meeting the US and Global regulatory standards (HIPAA, new consumer privacy laws[1] and HITRUST Certification requirements) and establishing the basis for a formal cybersecurit y framework (e.g., NIST, ISO27001, etc.)

In this digital age, criminals continue to attack medical community resources. Due to the sensitivity of electronic protected health information (ePHI), healthcare providers have increasingly complex fraud challenges and cybersecurity workforce issues as "bad actors" continue to refine their attacks. Without constantly implementing and reviewing data security measures, the chances of being breached increase exponentially. Moving information to Microsoft's protected Cloud services helps healthcare companies stay protected against new malicious code (i.e., malware) strains and reduces the chance that an unwanted email finds its way to an inbox. As such, Intraprise Health implemented Microsoft E5 licensing's security and compliance toolset to secure our own Microsoft 365 (M365) tenant.

A study was recently conducted by the U.S. Department of Health and Human Services on 2021 ransomware trends. The study revealed that the Health Sector Cybersecurity Coordination Center has tracked a total of 82 ransomware incidents impacting the healthcare sector worldwide so far this calendar year, as of May 25, 2021. Nearly 60% of these incidents. impacted the United States health sector. This makes ransomware one of the largest business challenges faced by the healthcare industry today, especially considering that the average bill for rectifying a ransomware attack is currently $1.27 million.[2]

Per HIPAA regulations, 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] can be combined with the M365 Security Center and the Compliance Center to enhance ePHI confidentiality, integrity, and availability. Part 2 of this whitepaper explores this concept in more detail.

Microsoft's investments in security, compliance, and auditing will be helpful to anyone interested in protecting data. Microsoft has integrated functions and provided clear lines of responsibility to support customer data protection. Additionally, M365 users can leverage built-in security and compliance features documented in Part 3 to achieve compliance for each aspect of the HIPAA Security Rule.

[1] California and New York City have implemented their own security and privacy bills called the California Consumer Privacy Act of 2018 and New York City Consumer Protection Law.
[2] Ransomware Trends 2021, U.S. Department of Health and Human Services, June 3, 2021. Also found here: https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf
[3] The National Institute of Standard and Technology (NIST) is the US Government Department that issues Federal cybersecurity and data security standards. They issue special publications which highlight methodologies the entire data security industry follows.

PART 1

HIPAA Regulations and Information Security Centric Features in the Microsoft 365 Platform

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 Microsoft 365.

Organizations in every industry, including the Department of Defense, are upgrading to Microsoft 365 to improve their security posture. Microsoft 365 has been designed to be the most secure cloud platform yet with architectural advancements built into every layer of the cloud computing stack.

However, as with all software upgrades, functionality, security, and privacy implications must be understood and addressed. It is critical that HIPAA Security Officers answer this question when potentially sending data to the cloud as part of its default operation, *"How does Microsoft 365 enable me to meet or exceed our HIPAA Security and Privacy requirement in my environment?".*

Microsoft has put tremendous focus on security and has the following global, regional, US and industry certifications:[4]

Azure, Dynamics 365, and Microsoft 365 compliance offerings

Information for Azure, Dynamics 365, Microsoft 365, and Power Platform, and other services to help with national, regional, and industry-specific regulations for data collection and use.

Global

- ☑ CIS Benchmark
- ☑ CSA-STAR attestation
- ☑ CSA-STAR certification
- ☑ CSA-STAR self-assessment
- ☑ ISO 20000-1:2011
- ☑ ISO 22301
- ☑ ISO 27001
- ☑ ISO 27017

Global

- ☑ ISO 27018
- ☑ ISO 27701
- ☑ ISO 9001
- ☑ SOC 1
- ☑ SOC 2
- ☑ SOC 3
- ☑ WCAG

USA Goverment

- ☑ CJIS
- ☑ CNSSI 1253
- ☑ DFARS
- ☑ DoD IL2
- ☑ DoD IL5
- ☑ DoE 10 CFR Part 810
- ☑ EAR (US Export Adm. Reg.)

USA Goverment

- ☑ FedRAMP
- ☑ FIPS 140-2
- ☑ IRS 1075
- ☑ ITAR
- ☑ NIST 800-171
- ☑ NIST CSF
- ☑ Section 508 VPATS

Industry

- ☑ 23 NYCRR Part 500
- ☑ A FIM + DNB (Netherlands)
- ☑ A PRA (Australia)
- ☑ A MF and ACPR (France)
- ☑ CDSA
- ☑ CFTC 1.31 (US)
- ☑ D PP (UK)
- ☑ EBA (EU)
- ☑ FACT (UK)
- ☑ FCA + PRA (UK)
- ☑ FDA CFR Title 21 Part 11

Industry

- ☑ FERPA
- ☑ FFIEC (US)
- ☑ FINMA (Switzerland)
- ☑ FINRA 4511 (US)
- ☑ FISC (Japan)
- ☑ FSA (Denmark)
- ☑ GLBA (US)
- ☑ GSMA
- ☑ GxP
- ☑ HDS (France)
- ☑ HIPAA / HITECH

Industry

- ☑ CIS Benchmark
- ☑ CSA-STAR attestation
- ☑ CSA-STAR certification
- ☑ CSA-STAR self-assessment
- ☑ ISO 20000-1:2011
- ☑ ISO 22301
- ☑ ISO 27001
- ☑ ISO 27017

Industry

- ☑ CIS Benchmark
- ☑ CSA-STAR attestation
- ☑ CSA-STAR certification
- ☑ CSA-STAR self-assessment
- ☑ ISO 20000-1:2011
- ☑ ISO 22301
- ☑ ISO 27001
- ☑ ISO 27017

Regional

- ☑ A BS OSPAR (Singapore)
- ☑ BIR 2012 (Netherlands)
- ☑ CS (Germany)
- ☑ Canadian Privacy Laws
- ☑ CCPA (US-California)
- ☑ Cyber Essentials Plus (UK)
- ☑ IRAP (Australia)
- ☑ CS Mark Gold (Japan)

Regional

- ☑ DJCP (China)
- ☑ EN 301 549 (EU)
- ☑ ENISA AIF (EU)
- ☑ ENS (Spain)
- ☑ EU Model Clauses
- ☑ GB 18030 (China)
- ☑ GDPR (EU)

Regional

- ☑ G-Cloud (UK)
- ☑ IDW PS.951 (Germany)
- ☑ ISMAP (Japan)
- ☑ ISMS (Korea)
- ☑ IT-Grundschutz workbook (Germany)
- ☑ LOPD (Spain)
- ☑ MeitY (India)
- ☑ MTCS (Singapore)

Regional

- ☑ My Number (Japan)
- ☑ NZ CC Framework (New Zealand)
- ☑ PASF (UK)
- ☑ PDPA (Argentina)
- ☑ Personal Data Localization (Russia)
- ☑ TRUCS (China)

[4] https://docs.microsoft.com/en-us/compliance/regulatory/offering-home

A common concern in the industry is that using Microsoft 365 opens an organization to HIPAA Security and Privacy violations. The truth is that M365 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 overarching 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 Security Rule – § 164.306(a) – requires healthcare organizations to:

1. Ensure the confidentiality, integrity, and availability of all electronically protected health information 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 PHI breach incidents as well as properly notify the specified parties

The HIPAA Privacy Rule ensures individuals have the minimum protections under the law. Incorrect configuration of modern operating systems and platforms, including M365, could violate the following laws and may lead to HIPAA non-compliance:

- Access to the Health Record – See patient rights §164.522, §164.524 §164.526
- Minimum Necessary Uses of PHI - See use and disclosure §164.514
- Content and Right to an Accounting of Disclosures – See privacy management process §164.528
- Business Associate Contracts – See privacy management process §164.504, §164.502, §164.524, §164.526, §164.528

A key component of HIPAA compliance today is the demonstration of appropriate IT-related internal controls designed to mitigate fraud, risk, and the implementation of safeguards for legally protected health information that is stored and transmitted in electronic form. 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 M365 Enterprise IT Security compliance for HIPAA.

See Appendix A for further review of HIPAA and associated regulations.

Information Security Centric Features in the Microsoft 365 Platform

In recent years, Microsoft has made tremendous information security improvements in what used to be called the Office 365 platform, now fully rebranded as Microsoft 365 or simply M365.

As Microsoft works to push more businesses towards cloud adoption, they have recognized the criticality of providing appropriate tools within the M365 boundaries for protecting the confidentiality, integrity, and availability of data stored in the Microsoft 365 Ecosystem. Tools such as BitLocker, Microsoft Defender, Windows Information Protection, Azure Active Directory, Azure Information Protection, Data Loss Prevention, and Data Sensitivity Labels work in concert to meet the core enterprise goals of managing data in a secure and auditable fashion.

Additionally, Microsoft has built two new portals as part of the E3/E5 licensing level (or available as add-ons to other M365 plans) that support many of the HIPAA Security Rule ePHI requirements. These two portals are called the Security Center and the Compliance Center, and they are found in their respective administrative portals within M365.

The Compliance Center (https://compliance.microsoft.com) is very well suited to common hardening and auditing requirements found in HIPAA. The Security Center, which can currently be found at https://security.microsoft.com, is all-new with tools for monitoring, reviewing and responding to security-related incidents and concerns (https://security.microsoft.com/homepage). On the main dashboard of the Security Center homepage are cards or widgets relevant to security-specific

metrics including Microsoft Secure Score, Microsoft Threat Protection, Users at Risk, Microsoft 365 Defender Feed.

The Secure Score is a particularly useful feature that provides an easy-to-digest, overall score of how the M365 Environment stacks up to the available security-specific tools and improvement actions that Microsoft has implemented and defined. The more improvement actions are implemented, the higher the Secure Score will climb. The available improvement actions are conveniently weighted to provide an understanding of their Secure Score impact.

Some of the improvement actions may be controversial, such as discontinuing the historically common practice of expiring user passwords at a set interval. This particular "improvement" is heavily weighted as Microsoft believes that expiring a user password (that should also be "complex") will lead to the user re-using the password elsewhere or simply writing it down in an easy-to-find location. Alternatively, there is the risk of a non-expired password getting "out in the wild", which could be disastrous if found by the wrong entity; however, when combining a non-expired password policy with a policy that enforces multi-factor authentication (MFA), then the risk is mitigated.

Other heavily weighted improvement actions are to enable sign-in risk policy and require MFA for administrative roles and ensure that users can enroll in MFA. Microsoft (and the rest of the InfoSec world) is making a push to move beyond single-factor authentication (i.e., something you know) to multi-factor authentication (i.e., something you know and something you have). A username and password combination are the most common "something you know" while verifying your identity with a smartphone MFA application or one-time password hardware token fulfills the "something you have" requirement.

There are currently 18 Microsoft 365 specific improvement actions that can be addressed within the Secure Score portal that will cumulatively work to increase a company's Secure Score. Microsoft allows organizations to drill down into each improvement action and provides additional information about where the specific controls are found within the M365 platform, to enable the actions and manage an action plan. The Secure Score portal is a great place to start to protect M365 Ecosystem data.

[1] https://www.congress.gov/116/bills/hr7898/BILLS-116hr7898eh.pdf
[2] https://www.hhs.gov/sites/default/files/hhs-ocr-hipaa-nprm.pdf
[3] https://www.hhs.gov/sites/default/files/hipaa-vaccine-ned.pdf
[4] https://public-inspection.federalregister.gov/2021-03348.pdf
[5] §164.308(a)(8)

PART 2

Microsoft 365: Data Security and HIPAA Compliance

With the constantly evolving proliferation of information security threats, combined with the complexity of meeting HIPAA regulatory mandates, healthcare organizations today need as many built-in compliance and security features as possible. The M365 Information Protection suite provides organizations with integrated turn-key security controls not previously available. It has never 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, meeting the confidentiality, integrity, and availability goals common to information security is now possible by leveraging tools built-in to the M365 platform. Encryption at rest can be achieved using BitLocker and BitLocker To-Go. Data integrity can be verified using digital signatures alongside Microsoft's Information Rights Management, while availability has been made possible by Microsoft's use of redundant hardware and data replication across many geographically diverse data centers.

Within the Compliance Center, which can be currently found at https://compliance.microsoft.com, organizations can now subscribe to premium templates for myriad compliance frameworks, including HIPAA. Once subscribed to a HIPAA compliance framework template, M365 provides a referenced audit and analyzes roughly 200 technical controls outlined in the template to score an organization. Additionally, Microsoft allows a user to "drill down" into each control to learn how and where to apply the control within the Microsoft 365 environment.

Introduction to Security in a Cloud-Enabled World

Cloud security 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 trustworthy cloud

Cybersecurity	Best-in-class security with decades of experience building enterprise software and online services.
Data Privacy	Privacy by design with a commitment to use customer's information only to deliver services and not for advertisements.
Compliance	Commitment to industry standards and organizational compliance.
Transparency	Visibility into how yourdata is handled and used, operational practices, Law Enforcement Reports, and Transparency Centers.

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

SaaS Software as a Service	PaaS Platform as a Service	IaaS 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. 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. You control access and secure your data, identities, and applications, including applying any infrastructure controls available from the cloud service. 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. 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.

Thanks to Microsoft, investments made implementing HIPAA from this whitepaper can be re-used to qualify for numerous U. S. and global standards and mandates in security controls[5].

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:

- Identitypolicies
- 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

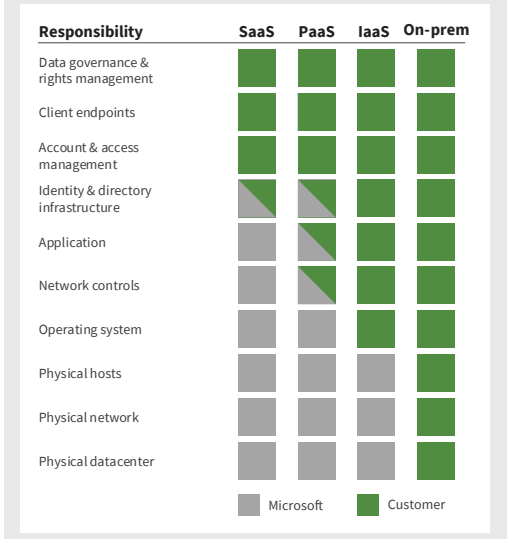
You own your data and control how it should be used, shared, updated, and published.

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.



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

The subscription used in this whitepaper is the Microsoft 365 E5 suite. The M365 E5 suite gives the maximum configuration of a HIPAA secure organization.

[5]Microsoft Cloud Architecture Security, Brenda Carter, Microsoft December 4, 20185

		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 Cloud PBX Required	Add-on Cloud PBX Required	Add-on	Add-on	$12/$24**

Security and Compliance for Microsoft 365

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

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

Security and Compliance Center

By leveraging Microsoft 365 E3 or E5 business subscription, organizations have access to a host of other tools including, Microsoft 365 Information Protection tools to manage Microsoft 365, Teams and other core Microsoft services.

Additional roles can be assigned to regular User Accounts (read: Domain Administrator-level access is NOT REQUIRED) to provide access and perform tasks in the Security and 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 view reports and settings of security features.

3. **Reviewer**
   Uses a limited set of analysis features in Microsoft 365 Advanced eDiscovery. Members of this group can see only the documents that are assigned to them.

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

5. **Organization Management**
   Members of this management role group have permission 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.

8. **Security Administrator**
   A 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 Security & Compliance Center. Members of this role group can use this section to review documents related to security, privacy, and compliance in Microsoft 365 to perform risk and assurance reviews for their own organization.

12 MailFlow Administrator

View 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 Microsoft 365 Security and Compliance Center is to be a one-stop portal for protecting all data in Microsoft 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 M365 and Teams organization, view the following resources:

- Manage your organization's Security and Compliance Administrative panel for Microsoft 365 and Teams
  https://protection.office.com
- Give users access to the Microsoft 365 Security & Compliance Center
  https://docs.microsoft.com/en-us/office365/securitycompliance/grant-access-to-the-security-and-compliance-center
- Permissions in the Microsoft 365 Security & Compliance Center
  https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center
- About Microsoft 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 the HIPAA Security regulations as selected by the Office for Civil Rights HIPAA Audit Protocol and provides guidance on customer's responsibilities with Microsoft 365 and Teams to meet HIPAA compliance and provide a solid foundation in data security controls.

PART 3

Microsoft 365, Teams, and HIPAA Traceability

With the explosive growth of cloud-usage and corresponding data communications, Intraprise Health has done extensive research on how to configure Microsoft 365 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 365 audit. Microsoft has undergone its own HIPAA Security and Privacy compliance assessment following their responsibilities as a business associate. In addition, Microsoft will provide Business Associate Agreements (BAA) for any Azure-enabled customer dealing with ePHI via the Microsoft Trust Center[6].

The following table provides insight regarding customer compliance with the HIPAA Audit Protocol[7] using Microsoft 365 while building a strong foundation of modern security controls. Failure to apply some recommended and documented hardening strategies for Microsoft 365 in a healthcare environment may expose organizations to potential HIPAA violations and potential penalties outlined in Part 1 above.

Accounts need to be configured to be used for verification and validation of the following controls. The accounts used must be granted these specific roles within the Microsoft 365 tenant to perform these duties:

- Compliance Administrator
- Global Reader
- Reports Reader
- Security Reader

The relationship between HIPAA citations and various Microsoft 365 features that satisfy those citations is complex. The table below indicates where there is a direct mapping from the HIPAA citation to an M365 feature. The absence of a "Y" in the table does not necessarily mean that M365 does not satisfy the citation. In some cases, many M365 features cross-reference to a single citation (as many as 30 or more), and Microsoft updates its feature set frequently. Attempting to list all possibly cross-references here would render the whitepaper obsolete in short order.

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

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

Customer-Managed HIPAA Controls for Microsoft Office 365 and Teams

HIPAA Citation	Category	Control Family	Key Activity	M365 Licensed Feature
§ 164.308(a)(1)(i)	Security Management Process	Administrative Safeguards	Prevent, detect, contain, and correct security violations	-
§ 164.308(a)(1)(ii)(A)	Risk Analysis	Administrative Safeguards	Assess potential risks and vulnerabilities	-
§ 164.308(a)(1)(ii)(B)	Risk Management	Administrative Safeguards	Reduce risks and vulnerabilities	-
§ 164.308(a)(1)(ii) ©	Sanction Policy	Administrative Safeguards	Apply sanctions against workforce members who fail to comply	-
§ 164.308(a)(1)(ii)(D)	Information System Activity Review	Administrative Safeguards	Review records of information system activity	Y
§ 164.308(a)(2)	Assigned Security Responsibility	Administrative Safeguards	Identify a security official	-
§ 164.308(a)(3)(i)	**Workforce Security**	**Administrative Safeguards**	**Ensure appropriate access to ePHI**	**Y**

HIPAA Citation	Category	Control Family	Key Activity	M365 Licensed Feature
§ 164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Administrative Safeguards	Implement procedures to authorize and supervise ePHI access	Y
§ 164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Administrative Safeguards	Determine that ePHI access is appropriate	-
§ 164.308(a)(3)(ii) ©	Termination Procedures	Administrative Safeguards	Terminate access to ePHI	Y
§ 164.308(a)(4)(i)	Information Access Management	Administrative Safeguards	Authorize access to ePHI consistent with the HIPAA Privacy Rule	Y
§ 164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions	Administrative Safeguards	Protect clearinghouse ePHI from unauthorized access	Y
§ 164.308(a)(4)(ii)(B)	Access Authorization	Administrative Safeguards	Grant access to ePHI information through used mechanisms	Y
§ 164.308(a)(4)(ii) ©	**Access Establishment and Modification**	**Administrative Safeguards**	**Establish, document, review, or modify a user's ePHI access to used mechanisms**	**Y**
§ 164.308(a)(5)(i)	Security Awareness and Training	Administrative Safeguards	Implement a security awareness and training program	-

HIPAA Citation	Category	Control Family	Key Activity	M365 Licensed Feature
§ 164.308(a)(5)(ii)(A)	Security Reminders	Administrative Safeguards	Provide periodic security updates	-
§ 164.308(a)(5)(ii)(B)	Protection from Malicious Software	Administrative Safeguards	Provide procedures to guarding against, detect, and report malicious software	Y
§ 164.308(a)(5)(ii)©	Log-in Monitoring	Administrative Safeguards	Provide procedures for monitoring and reporting log-in attempts	Y
§ 164.308(a)(5)(ii)(D)	Password Management	Administrative Safeguards	Provide procedures for creating, changing, and safeguarding passwords	Y
§ 164.308(a)(6)(i)	Security Incident Procedure	Administrative Safeguards	Address security incidents	Y
§ 164.308(a)(6)(ii)	**Response and Reporting**	**Administrative Safeguards**	**Identify and respond to security incidents**	**Y**
§ 164.308(a)(7)(i)	Contingency Plan	Administrative Safeguards	Respond to an emergency or other occurrence	-
§ 164.308(a)(7)(ii)(A)	Data Backup Plan	Administrative Safeguards	Create and maintain retrievable exact copies of ePHI	Y

HIPAA Citation	Category	Control Family	Key Activity	M365 Licensed Feature
§ 164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Administrative Safeguards	Establish procedures to restore any loss of data	Y
§ 164.308(a)(7)(ii) ©	Emergency Mode Operation Plan	Administrative Safeguards	Establish procedures to enable continuation of critical business processes	-
§ 164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Administrative Safeguards	Test and revise contingency plans	-
§ 164.308(a)(7)(ii) €	Applications and Data Criticality	Administrative Safeguards	Assess the relative criticality of specific applications and data	Y
§ 164.308(a)(8)	**Evaluation**	**Administrative Safeguards**	**Perform a periodic technical and nontechnical evaluation**	**Y**
§ 164.308(b)(1)	Business Associate Contracts and Other Arrangements	Administrative Safeguards	Obtain satisfactory assurances that Business Associates will appropriately safeguard ePHI	-
§ 164.308(b)(2)	Business Associate Contracts and Other Arrangements	Administrative Safeguards	Ensure Business Associates obtain satisfactory assurances from subcontractors	-
§ 164.308(b)(3)	Written Contract or Other Arrangement	Administrative Safeguards	Document business associate satisfactory assurances	-

HIPAA Citation	Category	Control Family	Key Activity	M365 Licensed Feature
§ 164.310(a)(1)	Facility Access Controls	Physical Safeguards	Limit physical access to ePHI systems and facilities	-
§ 164.310(a)(2)(i)	Contingency Operations	Physical Safeguards	Allow facility access in support of restoration of lost data	-
§ 164.310(a)(2)(ii)	Facility Security Plan	Physical Safeguards	Safeguard the facility and the equipment there in	-
§ 164.310(a)(2)(iii)	**Access Control and Validation Procedures**	**Physical Safeguards**	**Control and validate a person's access to facilities**	**-**
§ 164.310(a)(2)(iv)	Maintenance Records	Physical Safeguards	Document repairs and modifications to physical components affecting security	-
§ 164.310(b)	Workstation Use	Physical Safeguards	Specify workstations' functions, manner and physical attributes	-
§ 164.310©	Workstation Security	Physical Safeguards	Implement workstations' physical safeguards	-
§ 164.310(d)(1)	Device and Media Controls	Physical Safeguards	Govern hardware and electronic media receipt and removal	Y

HIPAA Citation	Category	Control Family	Key Activity	M365 Licensed Feature
§ 164.310(d)(2)(i)	Disposal	Physical Safeguards	Address ePHI and equipment final disposition	-
§ 164.310(d)(2)(ii)	Media Re-use	Physical Safeguards	Remove ePHI from electronic media	-
§ 164.310(d)(2)(iii)	**Accountability**	**Physical Safeguards**	**Maintain hardware and electronic media movements**	**Y**
§ 164.310(d)(2)(iv)	Data Backup and Storage	Physical Safeguards	Create a retrievable, exact copy of ePHI before moving equipment	Y
§ 164.312(a)(1)	Access Control	Technical Safeguards	Allow access only to those have been granted access	Y
§ 164.312(a)(2)(i)	Unique User Identification	Technical Safeguards	Assign unique credentials to track user identity	Y
§ 164.312(a)(2)(ii)	Emergency Access Procedure	Technical Safeguards	Obtain ePHI during an emergency	Y
§ 164.312(a)(2)(iii)	Automatic Logoff	Technical Safeguards	Terminate inactive sessions	Y

HIPAA Citation	Category	Control Family	Key Activity	M365 Licensed Feature
§ 164.312(a)(2)(iv)	Encryption and Decryption	Technical Safeguards	Encrypt and decrypt ePHI	Y
§ 164.312(b)	**Audit Controls**	**Technical Safeguards**	**Record and examine activity in information systems**	**Y**
§ 164.312(c)(1)	Integrity	Technical Safeguards	Protect ePHI from improper alteration or destruction	Y
§ 164.312(c)(2)	Mechanism to Authenticate ePHI	Technical Safeguards	Implement mechanisms to corroborate that ePHI has not been altered or destroyed	Y
§ 164.312(d)	Person or Entity Authentication	Technical Safeguards	Verify a person or entity seeking ePHI access is the one claimed	Y
§ 164.312(e)(1)	Transmission Security	Technical Safeguards	Guard against unauthorized ePHI access being transmitted	Y
§ 164.312(e)(2)(i)	Integrity Controls	Technical Safeguards	Ensure transmitted ePHI is not improperly modified	Y
§ 164.312(e)(2)(ii)	Encryption	Technical Safeguards	Encrypt ePHI being transmitted	Y

HIPAA Citation	Category	Control Family	Key Activity	M365 Licensed Feature
§ 164.314(a)(1)	**Business Associate Contracts and Other Arrangements**	**Organizational Requirements**	**Meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section**	**-**
§ 164.314(a)(2)(i)(A)	Business Associate Contracts	Organizational Requirements	Provide that a business associate will comply with applicable requirements	-
§ 164.314(a)(2)(i)(B)	Business Associate Contracts	Organizational Requirements	Ensure subcontractors that create, receive, maintain, or transmit ePHI agree to comply	-
§ 164.314(a)(2)(i)©	Business Associate Contracts	Organizational Requirements	Ensure business associate will report any security incident	-
§ 164.314(a)(2)(ii)	Other Arrangements	Organizational Requirements	Ensure another arrangement that meets Privacy Rule requirements	-
§ 164.314(a)(2)(iii)	Business Associate Contracts with Subcontractors	Organizational Requirements	Apply business associate contract requirements to subcontractors	-
§ 164.314(b)(1)	Requirements for Group Health Plans	Organizational Requirements	Safeguard ePHI on behalf of the group health plan	Y

HIPAA Citation	Category	Control Family	Key Activity	M365 Licensed Feature
§ 164.314(b)(2)(i)	**Group Health Plan Implementation Specification**	**Organizational Requirements**	**Implement safeguards to protect group health plan ePHI**	**Y**
§ 164.314(b)(2)(ii)	Group Health Plan Implementation Specification	Organizational Requirements	Ensure adequate separation is supported by security measures	Y
§ 164.314(b)(2)(iii)	Group Health Plan Implementation Specification	Organizational Requirements	Ensure any agent agrees to implement security measures	-
§ 164.314(b)(2)(iv)	Group Health Plan Implementation Specification	Organizational Requirements	Report any security incident to the group health plan	-
§ 164.316(a)	Policies and Procedures	Policies and Procedures and Documentation Requirements	Implement policies and procedures	-
§ 164.316(b)(1)	Documentation	Policies and Procedures and Documentation Requirements	Maintain the policies and procedures implemented	-
§ 164.316(b)(1)(ii)	Documentation	Policies and Procedures and Documentation Requirements	Maintain a record of actions, activities, or assessments	-
§ 164.316(b)(2)(i)	**Time Limit**	**Policies and Procedures and Documentation Requirements**	**Retain documentation for 6 years**	**-**

HIPAA Citation	Category	Control Family	Key Activity	M365 Licensed Feature
§ 164.316(b)(2)(ii)	Availability	Policies and Procedures and Documentation Requirements	Make documentation available	-
§ 164.316(b)(2)(iii)	Updates	Policies and Procedures and Documentation Requirements	Review and update documentation periodically	-

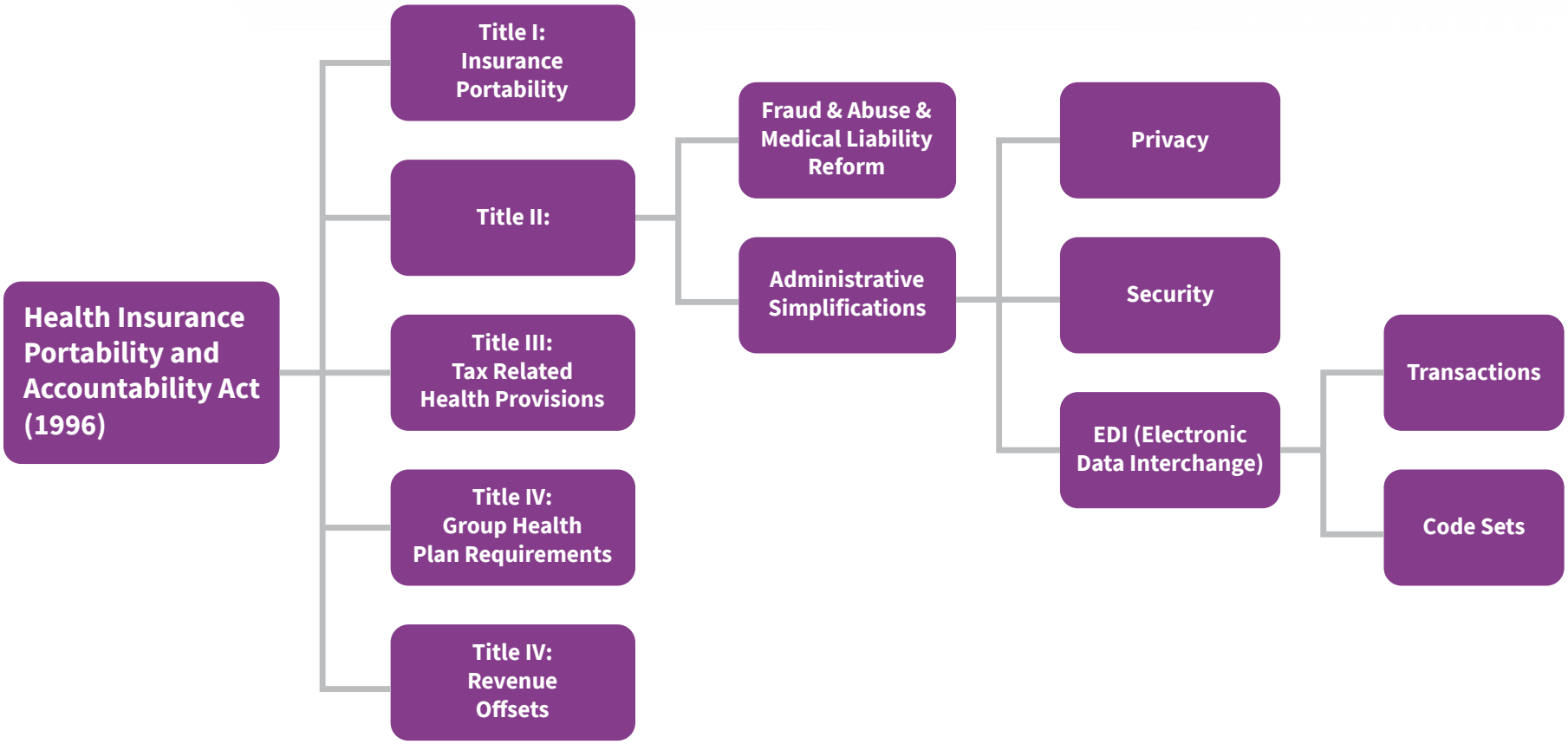
Document Version Control

Reviewed / Revision No	Date	Authorized Personnel	Summary of Change(s)
V2.0	8/12/2021	Intraprise Health, Proteus Consulting, and other contributors	Rewrite of whitepaper to current standards, updated Microsoft 365 feature links and terminology.

Appendix A

Health Insurance Portability and Accountability Act (HIPAA)

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.) The act was created because of the growing awareness that American citizens were not provided basic rights to their health information; specifically, the right to protect their personal information and retain a copy of their health records. Throughout the 1980s and 1990s, the federal government began receiving complaints stating they were not prepared to handle the mounting issue.



Early on, many clinics and hospitals were not open to sharing medical records with patients for several 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 announced 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 paper-based healthcare industry was experiencing skyrocketing costs. Pursuant to the American Recovery and Reinvestment Act (ARRA) passed in 2009, $29 billion was earmarked under the Health Information Technology for Economic and Clinical Health (HITECH) Act, (February 17, 2009), to provide both incentives to Covered Entities (hospitals and clinic-based doctors) and penalties in the form of Civil Monetary Penalties (CMP) for violating HIPAA Privacy, Security and Breach Notification Rules standards. 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 confidentiality, integrity and availability 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 HIPAA Security, Privacy, and Breach Notifications. This authority allowed the OCR to develop an audit standard, strategy, and process to respond to patient complaints.

Note that CMS renamed and updated the EHR Incentive Programs to the Promoting Interoperability Programs in April 2018. This change modernized Meaningful Use with an increased focus on interoperability and improving patient access to health information.

The HITECH Act, Security, and Privacy

As required by the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, 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 outlined that only NIST-based risk methodologies focused on security and compliance to the HIPAA rules were acceptable for conducting a bona fide HIPAA Security Risk Assessment and Analysis.

The HITECH Act extended HIPAA's traditional safeguard requirements directly to Business Associates of "Covered Entities." Covered Entities include hospitals, medical billing centers, health insurance companies, healthcare clearinghouses and other healthcare providers. The ruling expanded the HITECH Act's already broad "Business Associates" category, which includes health information exchange organizations, e-gateways handling ePHI and subcontractors that create, receive, maintain, or transmit protected health information on behalf of a business associate[9].

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 ePHI. In recent years, OCR has taken significant strides by imposing fines through settlements against providers who have failed to take reasonable and appropriate safeguards to protect their ePHI.

Specifically, HIPAA requires healthcare organizations to:

1. Ensure the confidentiality, integrity, and availability of all electronically protected health information 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 PHI breach incidents as well as properly notifying the specified parties

The HIPAA standard for audit controls states, "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."[10] To comply, organizations must have systems and processes that collect, store, alert, and report on non-compliant ePHI access, use, or disclosure (i.e., breach), thus creating the required audit trail and limiting ePHI disclosures to the minimum necessary.[11]

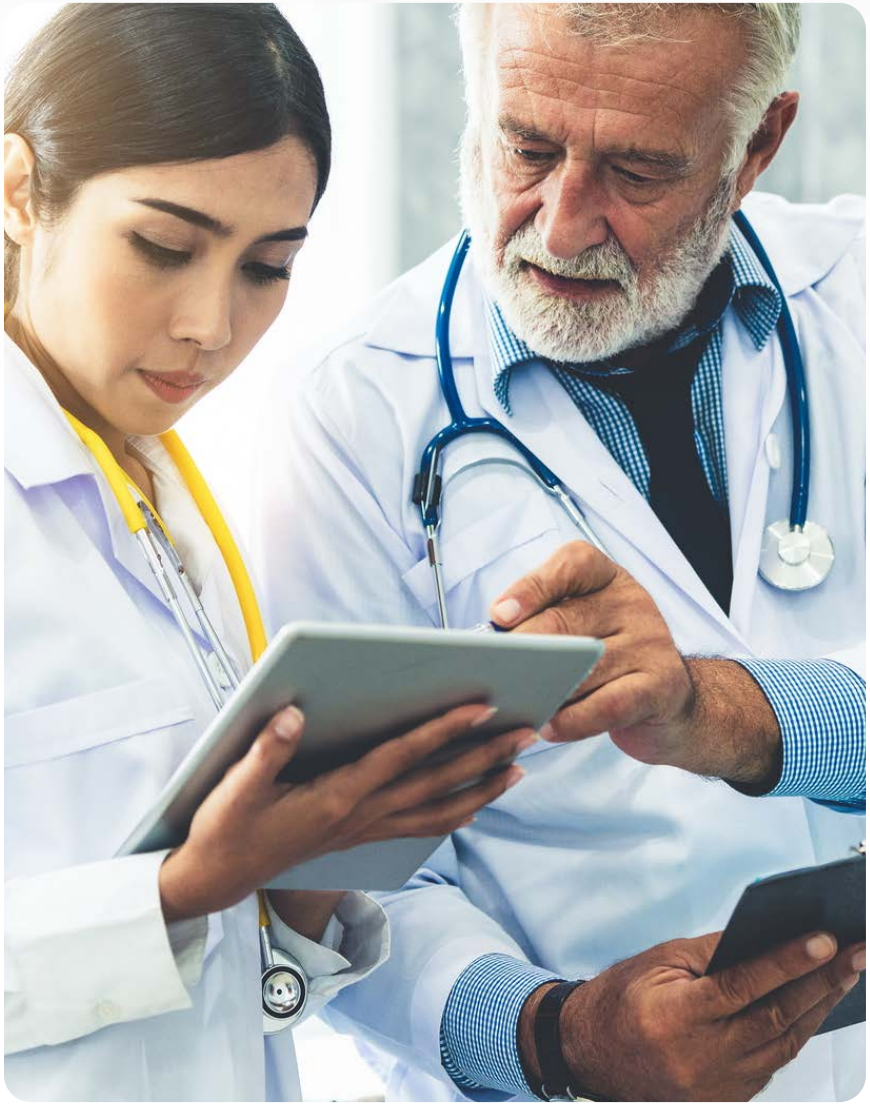
[8] HITECH Act Subtitle D, Section 13401.
[9] HITECH Act Subtitle D, Section 13408.
[10] 45 CFR § 164.312(b).
[11] 45 CFR § 164.514(d).

Under ARRA and HIPAA's Omnibus rule, virtually all organizations that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose ePHI must also comply with rigorous federal and state 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, there are additional rules that come into play, including notifying the media.[12]

ePHI 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



[12] HITECH Act Subtitle D, Section 13402.

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 voiceprints
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[13].

[13] 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.).

If a standard applies to ePHI, compliance is not optional. Strict adherence to specially marked implementation specifications, however, can be considered optional if, after an assessment is performed, they are determined to be "not reasonable and appropriate," the rationale to forgo the specification is documented, and evidence can be produced that a good faith effort was made to identify and implement "an equivalent alternative measure." Therefore, implementation specifications are categorized as either "required" or "addressable."

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

Addressable: If an implementation specification is marked as "addressable", it may be used to determine if it is "reasonable and appropriate." If deemed reasonable and appropriate to protect ePHI, it must be adopted and followed. If, however, a covered entity has determined that an "addressable" implementation specification is unreasonable or inappropriate for its environment, the entity should make a good faith effort to identify, implement, and document an equally effective alternative solution, or justify and document the decision to do neither.

While the databases of Electronic Health Record/Electronic Medical Record (EHR/EMR) systems are obvious areas where ePHI resides, there are many other systems in which ePHI may be stored or transmitted, including personal 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 regulations to protect all ePHI, however, is required. A table reflecting the penalty amounts for violations of HIPAA[14] as of 2021 follows:

Penalty Tier	Level of Culpability	Minimum Penalty per Violation 2021	Maximum Penalty per Violation 2021	Maximum Annual Penalty 2021
1	No Knowledge	$100	$50,000	$25,000
2	Reasonable Cause	$1,000	$50,000	$100,000
3	Willful Neglect – Corrective Action Taken	$10,000	$50,000	$250,000
4	Willful Neglect – No Corrective Action Taken	$50,000	$50,000	$1,500,000

The HIPAA Privacy Rule addresses protected health information in any medium, while the HIPAA Security Rule primarily covers the electronic medium. However, Covered Entities and Business Associates are bound by both sets of regulations. HIPAA requires the covered entity to protect/prevent exposure of previously listed 18 elements of specific data content, any element

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

of which might be exposed via email, file transfer, or other methods. Any/all other content outside of the 18 elements is not identified as Protected Health Information, so it is not subject to this HIPAA whitepaper. Other rules and regulations exist to also protect additional sensitive data categories (e.g., GDPR, FISMA, PCI, SOX, etc.).

Updates to HIPAA Rules

HIPAA Security Officers, whether operating from a dedicated compliance position or part-time as collateral or unanticipated additional duty, must keep abreast of Department of Health and Human Services (HHS) changes and significant information systems technology developments. HHS finalized their first changes to the HIPAA Rules in 2020 by updating the HITECH Act, has proposed changes to the HIPAA Privacy Rule, and published additional notices in the Federal Register affecting data sharing during the COVID-19 pandemic. While regulatory changes were promulgated, Microsoft continued maturing their cloud-based environment to Microsoft 365 in response to more organizations moving from legacy on-premise Microsoft services.

The HITECH Act was amended in January 2021 and directed the Secretary of Health and Human Services to "…consider certain recognized security practices of Covered Entities and Business Associates when making certain determinations, and for other purposes…"1. More specifically, this new amendment establishes some "safe harbor" conditions for Covered Entities and Business Associates that adequately demonstrate in-place recognized security practices developed under the National Institute of Standards and Technology Act and the Cybersecurity Act of 2015.

The OCR, the HHS enforcement agency, released a Notice of Proposed Rulemaking on January 21, 2021, to "…to increase permissible disclosures of PHI and to improve care coordination and case management…"2. OCR's proposed changes to the HIPAA Privacy Rule include:

- adding definitions, modifying individuals right of access to PHI
- creating a "minimum necessary" exception and clarifying PHI disclosures
- replacing "professional judgment" with a "best interests of the individual" disclosure permission
- expanding PHI disclosure to avert a threat to health or safety
- eliminating the Notice of Privacy Practice written acknowledgment
- permitting disclosures to Telecommunications Relay Services assistants, and
- expanding the Armed Forces permission to use or disclose PHI.

On January 19th, 2021, HHS released a notice of enforcement discretion stating that they "...will not impose penalties for non-compliance with regulatory requirements under the HIPAA Rules against covered health care providers or their Business Associates in connection with the good faith use of online or web-based scheduling applications for the scheduling of individual appointments for COVID-19 vaccinations during the COVID-19 nationwide public health emergency..."3. This notice of enforcement discretion was then updated on February 12th to limit this activity to "...a non-public facing online or web-based application that provides scheduling of individual appointments for services in connection with large-scale COVID-19 vaccination..."4.

Whether changes come about from compliance-based updates or technology, HIPAA Security Officers must determine whether such actions require updating their risk analysis in support of §164.308(a)(1)(ii)(A), performing an evaluation as required in §164.308(a)(8), or both. Critical to the evaluation process is technical testing "…in response to environmental or operational changes affecting the security of electronic protected health information…"5, which applies to establishing or change operating information services to the M365 Software as a Service (SaaS) platform. This testing verifies and documents that reasonable and appropriate technologies are properly configured to safeguard the confidentiality, integrity, and availability of electronic protected health information (ePHI).