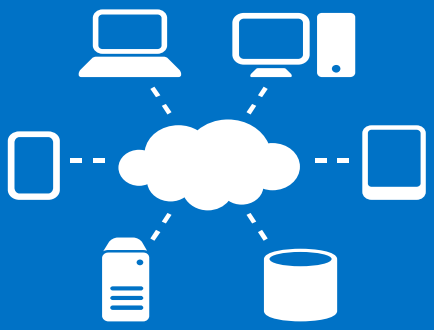
Addressing HIPAA Security and Privacy Requirements in the Microsoft Cloud



Authors
Mohamed Ayad, Microsoft Corporation
Hector Rodriguez, Microsoft Corporation
John Squire, Microsoft Corporation

Contributing Authors
SecureInfo Corporation, led by Yong Gon Chon

Microsoft

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2011 Microsoft Corporation. All rights reserved.

Microsoft, SQL Azure, Global Foundation Services, Office 365, and Dynamics CRM are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

CONTENTS

Executive Summary 5

Microsoft's Vision 6

Introduction 6

HIPAA and HITECH Primer: privacy, security and breach notification 8

- HIPAA and the HITECH Act 8
- Standards 9
- Implementation Specifications 9
- Protected health information or "PHI" 9
- Covered Entities 10
- Business Associates 10
- Business Associate Agreements 10
- Security obligations of a business associate 11
- What must a business associate require of its vendors? 11
- Breach notification obligations of a business associate 11
- Potential penalties for noncompliance with business associate obligations 11

The Real Threat to the Security and Privacy of ePHI 12

Embedding and Enabling Security in Microsoft's Cloud Infrastructure 14

Embedding and Enabling Security in Microsoft's Cloud Platforms and Services 16

- Microsoft's® Security Development Lifecycle (SDL) 17
- Security Best Practices For Developing Windows Azure Applications 18
- Automated Enforcement of Security Policies 19
  - Active Directory 19
  - Security Automation Tools 19
- HIPAA Compliance enabling Software Security Capabilities 22
  - Encryption 22
  - Protection of Data at Rest 23
  - Protection of Data in Transit 23

Identification and Authentication 24
Logging and Monitoring 24
Business Resiliency 25
Business continuity 25
Easy geo-availability 25
A financially backed SLA for Online Services 25
Microsoft is Your Trusted Data Steward 26
Earning your trust – Understanding the Problem Space 26
Enabling Compliance: Effective & efficient process-driven framework 26
Conclusion 27
References 28
Appendix A – Microsoft's Security Development Lifecycle 29
Training Phase 29
Requirements Phase 30
Design Phase 32
Verification Phase 33

EXECUTIVE SUMMARY

Organizations operating in the healthcare industry are continuously under pressure to use resources as efficiently as possible. They must provide innovation in patient care products and services enabled by advances in IT, and do so while maintaining compliance with an increasing burden of privacy and security regulations such as those posed by the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH).

Deploying Microsoft cloud and cloud enabled hybrid solutions[1] can give these organizations a method of focusing on patient care, while cost effectively consuming IT services, whether they are end-user applications or raw computing resources. On Microsoft's cloud, these solutions would use IT services as compliance enabling, secure, flexible and scalable utilities, rather than resource intensive, on-site, capital expenditures requiring on-going service and maintenance. Bottom line, the cloud gives healthcare organizations the opportunity to improve quality of care, access to care, increase services, and to reduce costs.

This whitepaper is aimed at business decision makers and IT managers at Covered Entities (hospitals, health plans, clearinghouses) and their Business Associates (defined by HIPAA as organizations that handle electronic Protected Health Information - ePHI). It provides a brief overview of regulation requirements, a detailed analysis of how Microsoft's cloud services were built with methodologies that map to those requirements, and guidance on how specific offerings can be incorporated by covered entities and their business associates into solutions that meet ongoing compliance needs that are subject to change over time.

[1] Cloud refers to Public, Private or a hybrid combination of both.

MICROSOFT'S VISION

Microsoft wants to be your Trusted Data Steward. We employ cutting edge technology complemented by years of experience, visionary research, and rigorous diligence, enabling you to address the implementation of technical, physical and administrative safeguards required by HIPAA. We do so by embedding security and privacy enabling functionality in our software to complement the security and privacy safeguards within our facilities and throughout our administrative processes. We can help you achieve and maintain compliance, while realizing the maximum benefits of your business decision to deploy solutions enabled by our cloud computing platforms and services.

INTRODUCTION

In today's environment, healthcare organizations face tough challenges in reducing cost and complexity while fostering innovation and collaboration. Healthcare providers must deliver high quality patient care, control spiraling costs, and proactively engage with their patients to improve population health. Health Plans must streamline their workflows and processes, and reduce infrastructure costs to meet their Medical Loss Ratio requirements. Software vendors catering to the healthcare industry want to differentiate their offerings through disruptive rather than incremental innovation. Last but not least, healthcare startups looking to scale their offerings to reach mass audiences are deterred by the cost and resource drain of provisioning and managing an IT infrastructure to match their growth aspirations.

These challenges are compounded by the need to comply with federal regulations, in particular those surrounding security and privacy where protected health information is concerned. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a U.S. federal law that mandates national standards to protect the privacy and security of health information, and the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") is a 2009 law that increases the obligations and penalties under HIPAA. These laws place the onus of compliance with security and privacy regulations in healthcare on the shoulders of what have been termed "covered entities" and by extension, their "business associates" or suppliers that come into contact with electronic Protected Health Information (ePHI).

A covered entity's compliance with these laws has so far proven troublesome with on-premise IT infrastructure. According to the data reported by the Department of Health and Human Services (DHHS), the vast majority of HIPAA breaches were a result of poor internal security, negligence, or petty theft - mainly of on-site physical assets[2].

The answer to the challenges of cost, complexity, innovation and collaboration lies in leveraging the power of the cloud. The cloud can deliver information and communication technology capabilities ranging from collaboration, knowledge management, communication and automation tools, to disaster recovery and high performance computing grids for research as a scalable, automated, high availability, low cost, low maintenance pay- as-you-go utility. A UC

[2] http://www.dhhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Berkeley study shows that moving to the cloud reduces infrastructure costs by a factor of 5 to 7, resulting in cost savings of up to 86% (Armbrust, et al., 2009).

However, healthcare organizations are reluctant to trust a third party with patient information. Decision makers are torn between their desire to take advantage of the financial and operational benefits of cloud computing and their concern over security and privacy of their data.

The solution is to work with a cloud platform provider that excels in the role of "Trusted Data Steward" as defined by the National Council for Vital Health Statistics (Kanaan & Carr, 2009), and that embeds compliance enabling security and privacy into its cloud offerings enabling adherence to administrative, technical, physical and organizational safeguards as specified in the HIPAA & HTECH provisions. In short, decision makers must work with a cloud provider that treats data as though they themselves are the covered entity.

The purpose of this whitepaper is to demonstrate how Microsoft, as a Trusted Data Steward enables and embeds security on its cloud infrastructure through its network of global data centers known as Global Foundation Services, cloud compute, storage and database platforms known collectively as the Azure platform, and cloud applications such as Office 365 and Dynamics CRM Online.

These technologies can be used by a covered entity's IT staff or its business associates to build compliance-ready solutions that allow the covered entity to focus on its primary goals. As Trusted Data Steward, we at Microsoft have enabled and embedded security in our technologies and employed a process-driven framework to help accomplish continuous compliance.

Working with Microsoft, decision makers are able to quickly grasp how to deliver cloud based solutions on top of Microsoft platforms that effectively protect the confidentiality, integrity and availability of ePHI, while safeguarding against anticipated security threats or hazards.

This paper is organized into five sections:

- Overview of HIPAA and HITECH privacy and security regulations
- Summary of HIPAA security challenges based on DHHS data
- Overview of how Microsoft enables and embeds security in its cloud infrastructure, platforms, and applications
- How Microsoft acts as Your Trusted Data Steward
- Enabling Ongoing Compliance – Effective & efficient process-driven framework

HIPAA AND HITECH PRIMER: PRIVACY, SECURITY AND BREACH NOTIFICATION

The expected audiences for this paper are business decision-makers, compliance managers, software development managers, IT consultants, and systems integrators who are working within or on behalf of organizations that must meet HIPAA and HITECH compliance requirements. **This paper is not intended to advise organizations of their legal requirements and responsibilities. It is assumed that the reader understands the laws and regulations mentioned in this paper and how those laws and regulations apply to their organization**. For readers unfamiliar with HIPAA and HITECH, we provide a very brief overview of these regulations. Readers already familiar with these regulations and their applicability to cloud solutions can skip ahead to The Real Threat to the Security and Privacy of ePHI.

HIPAA and the HITECH Act

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a U.S. federal law that mandates national standards to protect the privacy and security of health information. Title II of HIPAA was directed toward administrative simplification and included requirements for the Department of Health and Human Services (DHHS) to develop standards to standardize, facilitate, and secure electronic transmission of health data. The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") is a 2009 law that increases the obligations and penalties under HIPAA.

A full discussion of the historical background and specific requirements of HIPAA are beyond the scope of this paper. Interested readers may visit http://www.cms.hhs.gov/HIPAAGenInfo/.

The details about what HIPAA and the HITECH Act require are in the following three regulations:

- The HIPAA Privacy Rule, which limits the use and disclosure of protected health information ("PHI") and gives individuals privacy rights with respect to their PHI.
- The HIPAA Security Rule, which provides standards for *administrative, technical, and physical* safeguards to protect electronic PHI from unauthorized access, use, and disclosure in addition to organizational requirements such as Business Associate Agreements.
- The HITECH Breach Notification Interim Final Rule, which requires notice to be given to individuals and the government when a breach of unsecured PHI occurs.

These HIPAA rules apply to "covered entities" and their "business associates." They provide details on Standards and Implementation Specifications to be used in deploying security and privacy safeguards.

Standards

The use of the term standard can be confusing because it has numerous different uses in HIPAA and the Security Rule, including:

- The HIPAA statute which refers to Standard data elements or transactions, meaning that they comply with HIPAA-imposed requirements; for example, that something is a standard transaction.
- In the context of high-level HIPAA organization, in which Standard refers to the titles of the various regulations promulgated by DHHS; for example, Privacy Standards, Security Standards, or Transaction Standards. In this paper, we use the term Security Rule as opposed to Security Standards for clarity.
- The HIPAA Security Rule defines Standard, in pertinent part as "a rule, condition, or requirement" describing classification of components, specification of materials, performance, or operations, or delineation of procedures for products, systems, services, or practices. It is used to refer to a group of related requirements that must be met by Covered Entities; for example, the Security Management Process Standard. In this use a Standard is often a higher level requirement or a goal and often has one or more detailed sub-requirements, which are called Implementation Specifications.

Implementation Specifications

Implementation Specifications are specific processes to reach the goals established by the Standards. They may be either REQUIRED or ADDRESSABLE. A REQUIRED Implementation Specification must be met by the Covered Entity. An ADDRESSABLE Implementation Specification is not optional in the usual sense; Covered Entities must evaluate the practicality of each ADDRESSABLE Implementation Specification in terms of the security risk and the implementation cost and feasibility, in light of their own situation. If reasonable under the circumstances, such Implementation Specifications should be implemented as written. If deemed unreasonable, then an alternative approach should be implemented. The decision-making process must be documented.

Protected health information or "PHI"

"PHI" is a subset of health information, in any media, including demographic information collected from an individual, that is:

- created or received by a healthcare provider, health plan, employer, or health care clearinghouse;
- relates to an individual's health, provision of health care to the individual, or payment for the provision of health care; and
- identifies an individual or could reasonably be used with other available information to identify an individual.
- is not specifically excluded from the definition of PHI (generally, education, and employment records are excluded from HIPAA coverage)

PHI includes many common identifiers, such as name, address, and Social Security Number, and can be in any form or media, whether electronic, paper, or oral.

Covered Entities

HIPAA "covered entities" are:

- *health care providers* that engage in certain electronic transactions, including any health care provider that makes claims against a patient's health insurance;
- *health plans*, including health insurers and group health plans; or
- *health care clearinghouses*, which are entities that translate electronic health transactions formats.

As defined by CMS, software vendors are not identified as covered entities but they may, depending on the services offered and how they are used, be business associates to covered entities.

Business Associates

A "business associate" is an entity that accesses, uses, processes or discloses PHI on behalf of a covered entity for a service described in the HIPAA regulations. Microsoft's cloud services such as Azure, Office 365 and Dynamics CRM Online could make Microsoft a business associate when Microsoft provides these services to HIPAA covered entities if the covered entity were leveraging the online services to store and transmit PHI.

Business Associate Agreements

The HIPAA Privacy Rule and the HIPAA Security Rule require covered entities to obtain written assurances from their business associates that the business associates will appropriately safeguard the PHI they receive or create on behalf of the covered entity. These assurances typically are provided in a contract between the covered entity and business associate, known as a "business associate agreement."

Privacy obligations of a business associate

Business associate agreements must include certain requirements of the HIPAA rules. Specifically, business associates must:

- abide by the limitations on the use and disclosure of PHI set forth in the agreement;
- not use or further disclose PHI other than as permitted or required by the agreement or as required by law;
- use appropriate safeguards to prevent a use or disclosure of PHI other than as provided for by the agreement;
- comply with certain requirements with respect to individuals' right to access, amend, and receive an accounting of disclosures of PHI; and
- return or destroy PHI upon termination of the agreement.

Security obligations of a business associate

A business associate must comply with most provisions of the HIPAA Security Rule in the same manner as a covered entity. A business associate must first identify risks to its electronic PHI and may then consider such risks in the context of its size, complexity, technical infrastructure and capabilities and the costs of security measures. This analysis must then lead to the establishment of reasonable and appropriate measures to protect against such risks. The rule promotes a flexible approach to the satisfaction of the security requirements, with standards that are scalable, flexible, and technology-neutral.

The HIPAA Security Rule requires that a covered entity or business associate implement three types of safeguards (mechanisms, processes, or procedures used to mitigate security vulnerabilities and reduce security risks) to protect electronic PHI:

- administrative safeguards (e.g., security management process, security awareness training);
- physical safeguards (e.g., facility access controls, device and media controls); and
- technical safeguards (e.g., access control, transmission security).

These security measures must be documented and kept current, and the business associate must retain such documentation for at least six years.

What must a business associate require of its vendors?

Business associates must ensure that any agents, vendors or subcontractors they provide PHI to agree to the same restrictions and conditions that apply to the business associates with respect to PHI.

Breach notification obligations of a business associate

The HIPAA Breach Notification Rule requires business associates notify covered entities following the discovery of a breach of unsecured (i.e., unencrypted) PHI. This notification must be made without unreasonable delay and in no case later than 60 days after discovery of the breach—but the business associate agreement may require a shorter time frame. The rule also requires that business associates have in place reasonable measures to detect breaches of unsecured PHI.

Potential penalties for noncompliance with business associate obligations

A business associate may be subject to civil and criminal penalties for violations of HIPAA. Civil penalties range from $100 to $50,000 per violation, depending on the nature of the violation, with a cap of $1.5 million for all identical violations in a calendar year. Criminal penalties include fines ranging up to $250,000, imprisonment ranging up to 10 years, or both, depending on the type of violation. A business associate may also be contractually liable to the covered entity for breaches of the business associate agreement.

THE REAL THREAT TO THE SECURITY AND PRIVACY OF EPHI

For many business decision makers at many healthcare organizations, the "cloud" conjures up multiple misconceptions about security, privacy, and sovereignty over data. Based on interviews with management at covered entities, Microsoft has seen concerns categorized as follows:

1. Keeping data secure

"I can't have patient data on outside servers."

2. Losing Control

"Even if Microsoft is running it, I'm still on the hook"

3. Legal concerns

"Our lawyers would never allow it"

The reality today is that ePHI is being stored outside the covered entities' walls, and legal departments are agreeing to this decision based on the security and privacy measures that hosting vendors demonstrate, and the financially backed SLA's that they provide. However, it is important to gain a true understanding of the real threats to the security and privacy of ePHI. The HITECH Act in section 13402 (e)(4) requires that the Secretary of the DHHS post a list of breaches of unsecured PHI that affect 500 or more individuals.

As of the 14th of September 2011, there were 358 breaches of security. These involved one or more types of breach, from one or more locations or devices. Analysis of these breaches reveals interesting insights. The following tables summarize the frequency of these breach types, and where they took place.

Breach Type	Number	% of Total
Theft	194	54%
Unauthorized Access/Disclosure	82	23%
Loss	54	15%
Hacking/IT Incident	30	8%
Improper Disposal	21	6%
Unknown	5	1%
Other	1	0%

Table 1. Types of Breaches of ePHI involving more than 500 individuals (DHHS)[3]

[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Breach Location/Device	Number	% of Total
Paper	88	25%
Laptop	88	25%
Computer	64	18%
Other Portable Electronic Device	61	17%
Network Server	43	12%
Other	21	6%
Electronic Medical Record	9	3%
E-mail	9	3%
Backup Tapes	4	1%
Hard Drives	3	1%
Mailings	2	1%
CDs	1	0%

Table 2. ePHI storage Location/Device breached involving more than 500 individuals (DHHS)[4]

Closer inspection of publicly available records pertaining to the largest breaches to date shows the following:

Covered Entity	Year	Records Affected	Breach Description
Health Net	2011	1,900,000	Disks stolen or missing from Health Net's datacenter.[5]
NYC Health & Hospitals Corporation	2010	1,700,000	Hard drives containing PHI stolen from a van.[6]
AvMed	2009	1,220,000	Laptops stolen from the corporate office in Gainesville.[7]
Blue Cross Blue Shield	2009	1,023,209	Hard drives containing PHI stolen from an IT network closet.[8]
South Shore Hospital	2010	800,000	Disk drives were lost when being transported to a contractor for destruction.[9]

[4] ibid
[5] http://www.dmhc.ca.gov/aboutthedmhc/itn/itn_press.aspx
[6] http://www.nyc.gov/html/hhc/html/pressroom/pr-20110211-data-theft.shtml
[7] http://www.avmed.org/pdf/unsecure/Press%20Room/Press%20Releases/10/2010-01-08_AvMed_Breach_Release.pdf
[8] http://www.bcbst.com/about/news/releases/default.asp?release=311
[9] http://www.southshorehospital.org/news/notice/news_statement.htm

As seen from the data, the number one threat to the security of ePHI is theft, followed by unauthorized access/disclosure from on-premise resources. Stolen laptops or paper records together account for 50% of breaches out of the reported total.

The conclusion to be drawn from the data is that, as of the date of publication of this paper, none of these breaches occurred in a secure public cloud environment, where strict physical, technical, and administrative safeguards are in place.

Thus, decision makers who are serious about demonstrating their efforts at lowering their exposure to costly and damaging breaches of security *must* consider the benefits of transitioning to Microsoft's secure cloud platforms.

EMBEDDING AND ENABLING SECURITY IN MICROSOFT'S CLOUD INFRASTRUCTURE

Microsoft's approach to privacy and security is foundational, and starts with securing the cloud infrastructure. Microsoft operates a global network of industry leading datacenters incorporating extensive physical safeguards

Microsoft's Facilities Access Controls and automated server management systems help ensure that the leading causes of HIPAA security breaches such physical thefts of hard drives and laptops become a virtual non-issue for organizations transitioning to the Microsoft cloud. If individual physical copies of ePHI must be maintained, the use of Microsoft's Bitlocker and AD RMS can ensure that these copies are managed securely.

PHYSICAL:
- Strict access control
- Biometric scanning
- Video surveillance
- Redundant power supplies from separate providers
- Battery & diesel backup generators
- Climate control
- Fire prevention & suppression

Microsoft's cloud infrastructure security is operated by the Online Services Security and Compliance (OSSC) team within Microsoft's Global Foundation Services Division. This team builds on the same security principles and processes that Microsoft has developed through years of experience managing security risks in traditional development and operating environments.

DATA & NETWORK:
- Security monitoring
- Threat & vulnerability mgmt
- Access Control, file/data integrity
- Dual-factor authorization
- Intrusion detection
- Anti-malware, patch management
- Edge Routers and FW

The OSSC team within GFS is responsible for the Microsoft cloud infrastructure Information Security Program, including policies and programs used to manage online security risks. The mission of OSSC is to enable trustworthy online services that create a competitive advantage for Microsoft and its customers.

Placing this function at the cloud infrastructure layer allows all Microsoft cloud services to take advantage of economies of scale and reduced complexity through use of shared security solutions. Having this standard approach also enables each of the Microsoft service teams to focus on the unique security needs of their customers.

The OSSC team drives the effort to provide a trustworthy experience in the Microsoft cloud through the Microsoft Information Security Program using a risk-based operating model and a defense-in-depth approach to controls. This includes regular risk management reviews, development, and maintenance of a security control framework, and ongoing efforts to ensure compliance in activities ranging from data center development to responding to requests from law enforcement entities.

The team applies best practice processes, including a variety of internal and external reviews, throughout the lifecycle of online services and each element in the infrastructure. Close working relationships with other Microsoft teams result in a comprehensive approach to securing applications in the Microsoft cloud.

Operating a global cloud infrastructure across many businesses comes with the need to satisfy compliance obligations and to withstand the scrutiny of outside auditors. Auditable requirements come from government and industry mandates, internal policies, and industry best practices. The OSSC program ensures that compliance expectations are continuously evaluated and incorporated.

As a result of the Information Security Program, Microsoft is able to obtain key certifications such as Statement of Auditing Standard (SAS) 70 Type I and Type II attestations and International Organization for Standardization / International Society of Electrochemistry 27001:2005 (ISO/IEC 27001:2005), and to more efficiently pass regular audits from independent third parties.

COMPLIANCE & CERTIFICATION:

- SAS 70 compliant
- ISO 27001 compliant
- FISMA compliant
- Industry certification core part of Microsoft services roadmap
- Additional certification applications in process

ISO 27001 is a specification for an Information Security Management System (ISMS), meaning the system for monitoring, measuring and controlling information security as a whole. It explains how to apply the controls within ISO 27002 (formerly known as ISO 17799) which is a code of practice for information security management.

Microsoft's ISO certification for its data centers can be viewed here

More information can be found here:
Microsoft's Online Services Trust Center
Microsoft's Azure Trust Center

These certifications are especially significant in the context of healthcare, as there are currently no certification bodies for HIPAA. However, the aforementioned certifications cover a large segment of the safeguards specified in HIPAA law.[10]

[10] http://www.zygma.biz/pdf/Zygma%20-%2017799%20vs%20HIPAA%20white%20paper%20v1bis.pdf

EMBEDDING AND ENABLING SECURITY IN MICROSOFT'S CLOUD PLATFORMS AND SERVICES

Microsoft makes the distinction between Software as a Service, Platform as a Service and Infrastructure as a Service when approaching HIPAA privacy and security safeguards. For a number of Microsoft's SaaS offerings, such as Office 365 and Dynamics CRM Online, Microsoft currently signs a Business Associate Agreement with covered entities, supporting compliance with safeguards that protect the privacy and security of ePHI. With these safeguards in place, covered entities can implement policies and procedures that support their responsibility for end-to-end compliance with HIPAA and HITECH.

By contrast, ePHI stored on IaaS, or PaaS offerings such as Windows Azure which provides compute and non-relational storage capabilities, and SQL Database (formerly known as SQL Azure), which provides relational database capabilities are by definition subject to the software development and implementation practices of the organizations that use them, in addition to required policies and procedures that might have been sufficient to support compliance in a SaaS setting. Microsoft has implemented the physical, technical and administrative safeguards required by HIPAA and HITECH for Windows Azure Core Services and now offers a Business Associate Agreement for those services. Additionaly, Microsoft maintains a compliance roadmap that is discussed with partners and customers around Microsoft's ability to sign a BAA for the different Azure platform components, and the applicability of Business Associate Agreements for particular architectures of solutions built on Azure.

Microsoft Services covered by a Business Associate Agreement

Dynamics CRM Online Services

Office 365 Services

- Exchange Online
- Exchange Online Archiving
- Sharepoint Online
- Lync Online
- Office Web Apps

Windows Azure Core Services

- Windows Azure Cloud Services (web and worker roles),
- Storage (blobs, tables, queues),
- Virtual Machines
- Networking (Windows Azure Connect, Traffic Manager, Virtual Network)

Microsoft's deep understanding of this subtlety stems from working with organizations such as the HITRUST Alliance, implementing the Common Security Framework for Covered Entities privacy and security requirements. This collaboration results in Microsoft's restraint from claiming "HIPAA compliance" for Azure platforms and Microsoft Online Services. However, Microsoft asserts that the Azure platform and Online Services capabilities "enable and support compliance" by covered entities. Covered entities, responsible for their end-to-end compliance on the cloud, can architect solutions on the Azure platform that comply with HIPAA safeguards and can use Online Services, with the right administrative safeguards, policies and procedures in place that would ensure their compliance with HIPAA.

Moreover, Microsoft's approach to privacy and security integrates safeguards into how its cloud software platforms are initially developed. This is done using Microsoft's® Security Development Life Cycle, a set of processes and best practices that incorporate security and compliance throughout each step of the development process. Microsoft encourages application developers to adopt the Security Development Lifecycle into their own application development efforts, thereby standardizing security throughout the full architecture of their end

solutions. An analysis conducted in November 2010 shows that Microsoft's SDL processes aligns with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule 45 CFR Part 169 and Part 164.
http://www.microsoft.com/download/en/confirmation.aspx?id=11942

Microsoft has taken additional steps that differentiate security and privacy measures in the cloud over competing platforms. These steps include providing automated security policies in their cloud products through robust configuration options, comprehensive logging and auditing features, capabilities for strong encryption such as Azure Trust Services encryption for data-at-rest and Forefront Online Protection for Exchange for data-in-motion, documented identification and authentication policies, around-the-clock security monitoring. Moreover, Microsoft provides organizations with widely-available HOW-TO guidance via Technet articles, and is committed to delivering secure, private, and reliable cloud computing through their Trustworthy Computing Initiative.

The details of these 3 processes and technologies will be covered in this section:

- Microsoft's Secure Development Lifecycle, used in the development of our cloud solutions
- Our internal, automated security policies used in Microsoft datacenters that host our cloud solutions
- HIPAA Compliance enabling Software Security Capabilities, the technology embedded in our cloud solutions

Readers not interested in these details can skip ahead to the section on "Business Resiliency".

Microsoft's® Security Development Lifecycle (SDL)

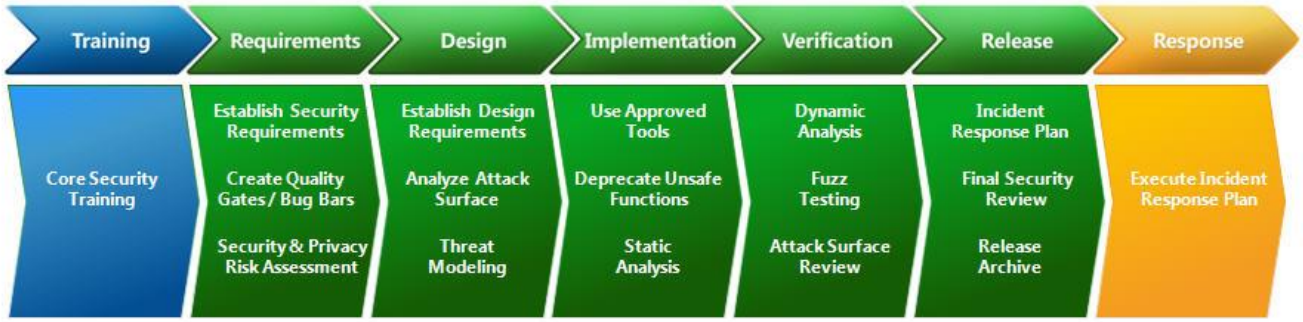


Figure 1: The SDL process

When covered entities deploy a solution enabled by a Microsoft cloud service offering, they are assured that security is built-in to the software product throughout its development process. Microsoft has designed a software development security assurance process that consists of a

collection of security practices, grouped by the phases of the traditional software development life cycle. When executed in chronological order as part of a repeatable process, these practices result in measurably greater standards of security than those resulting from ad hoc software development.

The SDL toolset and/or accompanying consulting services can be adopted by software developers and is the methodology that all of Microsoft's services offerings follow to ensure secure coding and compliance of Microsoft products. Microsoft's cloud platforms were designed using the Security Development Lifecycle,

The Microsoft SDL is based on three core concepts—*education, continuous process improvement, and accountability*. The ongoing education and training of technical job roles within a software development group is critical. The appropriate investment in knowledge transfer helps Microsoft and its partners to react appropriately to changes in technology and the threat landscape. Because security risk is not static, the SDL places heavy emphasis on understanding the cause and effect of security vulnerabilities and *requires* regular evaluation of SDL processes and introduction of changes in response to new technology advancements or new threats. Data is collected to assess training effectiveness, in-process metrics are used to confirm process compliance and post-release metrics help guide future changes. Finally, the SDL requires the archival of all data necessary to service an application in a crisis. When paired with detailed security response and communication plans, an organization can provide concise and cogent guidance to all affected parties.

As depicted in the figure above, the SDL is broken down into seven component areas; however there are five capability core areas that roughly correspond to the phases within a traditional software development cycle:

- Training, policy, and organizational capabilities
- Requirements and design
- Implementation
- Verification
- Release and response

Out of the five core SDL areas, four of these phases map directly to requirements set forth in the HIPAA Security Rule. These four phases are furthered explained in Appendix A. For a full discussion of how Microsoft's SDL processes align HIPAA Security Rule 45 CFR Part 169 and Part 164, please review this whitepaper:

SDL and HIPAA - Aligning Microsoft SDL Security Practices with the HIPAA Security Rule

The following whitepaper describes some of the security technologies software developers should use, and the security design and development practices they should use to build more secure Windows Azure applications

Security Best Practices For Developing Windows Azure Applications

Automated Enforcement of Security Policies

When healthcare organizations deploy solutions enabled by Microsoft cloud products, they are inheriting from Microsoft all of their automated enforcement of security policies through Active Directory and their host of vulnerability scanning and patching tools.

Active Directory

Microsoft product teams use Active Directory Domain Services (ADDS), as the central location for configuration information, authentication requests, and information about all of the objects that are stored within the AD forest of trusted domains. By using Active Directory, Microsoft product teams can efficiently manage users, computers, groups, applications, and other directory-enabled objects from one secure, centralized location.

Active Directory Group Policy settings are utilized by Microsoft product teams to enforce security policies such as password expiration, complexity, length, history, and reusability. Active Directory security settings are configured to inhibit attempts to gain unauthorized access to resources in the domain. These configurations require users to have a unique identifier for their individual use only, the use of appropriate authentication techniques to substantiate the claimed identity of a user, and system log-in procedures that minimize disclosure of information about the system in order to avoid assisting individuals attempting to gain unauthorized access. Active Directory group policies are also configured to ensure the integrity of member servers in their domain by pushing out clock synchronization via domain controllers. Additional security mechanisms provided by Active Directory restrict access and log activities.

For Microsoft's multitenant cloud solutions, Active Directory Organizational Units (OUs) control and prevent the unauthorized and unintended information transfer via shared system resources. Tenants are isolated from one another based on security boundaries, or silos, enforced logically through Active Directory.

In addition to Active Directory Domain Services, Microsoft cloud products offer enhanced base capabilities for healthcare users by supporting integration with Active Directory Rights Management Services. Active Directory Rights Management Services (AD RMS) helps Covered Entities and Business Associates (BAs) make sure that only those individuals who need to view ePHI can do so. AD RMS can protect a file by identifying the rights that a user has to the file. Rights can be configured to allow a user to open, modify, print, forward, or take other actions with the rights-managed information. With AD RMS, healthcare providers can now safeguard data when it is distributed outside of the network.

Security Automation Tools

All of Microsoft's cloud services subscribe to Microsoft's Security Response Service to receive security updates, bulletins, and advisories. The Microsoft Security Response Center (MSRC) is a global team dedicated to ensuring safety when using Microsoft products. The MSRC delivers security updates and authoritative security guidance to Microsoft and Microsoft customers. The MSRC identifies, monitors, resolves, and responds to security incidents and Microsoft software vulnerabilities. The MSRC also manages Microsoft company-wide security update release processes and serves as the single point of coordination and communications. The MSRC

releases security bulletins on the second Tuesday of every month. Subscribers to the Microsoft Security Bulletin Advance Notification receive advance notification three business days before the regular security update release on the second Tuesday of the month, which aids Microsoft product teams in configuring their infrastructure monitoring tool, QualysGuard. Microsoft cloud services employ numerous security automation tools to assist in identifying and remediating risks. Security automation uses vulnerability scanning, patching, anti-virus, compliance, reporting and ticketing tools.

Vulnerability scanning tools such as QualysGuard verify the status of security updates in the cloud infrastructure environment. QualysGuard is an application that performs host and application level vulnerability assessments on a daily basis. The tool is updated frequently to meet the demands of the ever-changing threat environment. Additional vulnerability tools are employed for web application and database scanning. Microsoft's diligence in performing vulnerability management directly benefits covered entity customers that develop on the Microsoft cloud platform as their systems will be scanning regularly. The following table shows which Qualysguard capabilities help meet which HIPAA requirements. Customers and partners working with Microsoft cloud products should conduct their own risk assessments as well.

HIPAA / HITECH Requirements	Microsoft's QualysGuard Implementation
Security Management Process. a. 164.308(a)(1) b. 164.308(a)(1)(ii) c. 164.308(a)(1)(ii)(A) d. 164.308(a)(1)(ii)(D)	QualysGuard's Vulnerability Management and Policy Compliance solutions underpin security management with a complete, automated system for security audits and IT compliance management.
Information Access Management. a. 164.308(a)(4) b. 164.308(a)(4)(ii)(A) c. 164.308(a)(4)(ii)(B)	Audits user access to systems and databases containing PHI.
Security Awareness and Training. a. 164.308(a)(5) b. 164.308(a)(5)(ii)(B) c. 164.308(a)(5)(ii)C d. 164.308(a)(5)(ii)(D)	Security and configuration data revealed by QualysGuard reporting capabilities help staff and management with their network security posture and how to further protect it against emerging threats.
Security Incident Procedures. a. 164.308(a)(6)	Security and configuration audit assessments provide hard data for conceiving, implementing, and managing security policies.
Evaluation. a. 164.308(a)(6)	Automatically and regularly tests and documents security capabilities and configuration settings before and after installation and maintenance of networks, systems, or applications.

HIPAA / HITECH Requirements	Microsoft's QualysGuard Implementation
Workstation Security. a. 164.310(C)	QualysGuard automatically and regularly tests and documents security capabilities and configuration settings before and after installation and maintenance of networks, systems, or applications.
Device and Media Controls. a. 164.310(d)(2)(i) b. 164.310(d)(2)(iv)	Tests and documents configuration settings automatically before and after installation and maintenance of networks, systems, or applications.
Access Control. a. 164.312(a)(1)	Audits user access to systems and databases containing PHI.
Audit Control. a. 164.312(b)	Automatically and regularly tests and documents configuration settings before and after installation and maintenance of networks, systems, or applications.
Integrity. a. 164.312(c)(1) b. 164.312(c)(2)	Audits user access to systems and databases containing PHI.
Transmission Security. a. 164.312(e) b. 164.312(e)(1)	Audits transmission settings on systems, thus validating secure transmission of PHI.

Table 1-1: QualysGuard mapping to HIPAA requirements

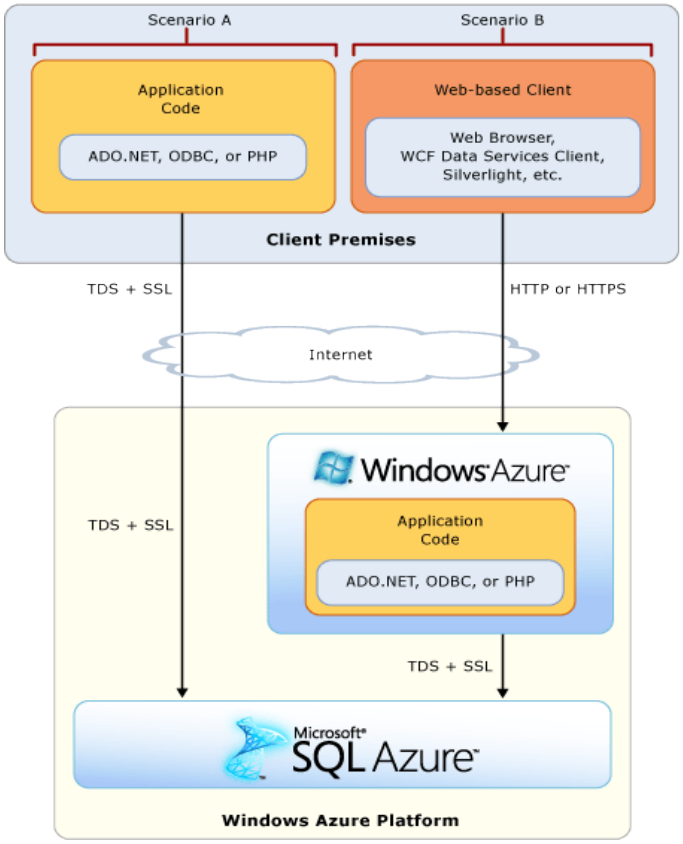
Microsoft product teams use a wide variety of remediation tools to assist in applying patches and applicable security updates. The tools used are scalable for large organizations such as the cloud environment and have reporting capabilities on a device-by-device basis. All security updates and patches must go through the SDL process and rigorous testing before deployment into the production cloud environment.

Anti-virus software is deployed on all servers in the Microsoft cloud environment as malicious software protection. The anti-virus software utilized by Microsoft cloud services supports a fully centrally managed solution that includes scanning real-time files incoming to the systems, automatic checks for updates signature files and software updates, and alerts to Microsoft's Operations Center (MOC) of detected malicious code.

Microsoft product teams use compliance tools to help track the numerous compliance certifications and attestations each product team has achieved, one of which is support for HIPAA compliance. These tools help product teams maintain and enforce security policies throughout the cloud environment.

HIPAA Compliance enabling Software Security Capabilities

Security is often the last item thought of when developing applications and technology systems. At Microsoft, we have embedded numerous controls into our cloud infrastructure and platforms that ensure that safeguards are never forgotten. Embedding safeguards begins with information classification. Microsoft classifies information based on business impact so that sensitive information may be well protected, managed, and monitored with appropriate controls. The following whitepaper describes Microsoft's approach that covered entities can leverage for classifying their information.



[Securing Business Information Work Smart Guide]

Encryption

Microsoft offers a wide range of cryptographic solutions within the cloud and has been a thought leader in offering cryptographic libraries to its customers for years. Currently, Microsoft holds 49 separate FIPS 140-2 validated certificates for its encryption work which offers protection to not only to sensitive information that Microsoft houses, but also to its application developer community using Microsoft platforms, technology and cloud services.

Resources:

How Do I Use Smart Encryption Techniques for Cloud Apps?

FIPS Validated Cryptographic Libraries

Protection of Data at Rest

The Windows Azure SDK extends the core .NET libraries to allow the developer to integrate and make use of the services provided by Windows Azure. This means that developers will have access to the full array of .NET cryptographic services in Windows Azure. These are vital to enhance the security of any system for protecting data at rest. By leveraging the SDK, developers at covered entities or their business associates can enforce policies and procedures necessary for HIPAA and ensure mechanisms implemented for encrypting sensitive data in storage.

One of the tools that Microsoft is developing to aid with securing of ePHI at rest through encryption or de-identification is the Azure Trust Services.

Microsoft Codename "Trust Services" is an application-level encryption framework that can be used to protect sensitive data stored on the Windows Azure Platform. Data encrypted with Trust Services can only be decrypted by authorized data consumers. This empowers data publishers to freely distribute and share data by first encrypting using the Trust Services. Consumers of or subscribers to sensitive data encrypted with Trust Services can have a measure of confidence in the integrity of the data and the knowledge that the risk of unauthorized access to the data is minimized.

The basic scenario involves 2 steps:
• Data producers use Trust Services to encrypt sensitive data and store it in Windows Azure storage or SQL Azure
• Authorized data consumers can decrypt data after it is read from storage

Only "publishers" and "subscribers" to the data hub can encrypt or decrypt data based on policy set by the application administrator. The trust services module itself is not "trusted" with the encryption keys. Therefore Microsoft has no access to keys required to decrypt the encrypted data columns, and the application developer can architect to ensure that sensitive data such as identifier fields in a health record will never reside on Microsoft systems except in an encrypted fashion and that Microsoft (our systems, and employees, vendors etc.) will virtually never have the means to decrypt that data.

Protection of Data in Transit

Developers benefit from numerous data in transit features available in Microsoft's cloud offerings. At the highest level, connections across the Internet leverage SSL encryption supporting a wide range of ciphers that can ensure Internet connection privacy and integrity.

Additionally, SQL Azure supports the tabular data stream (TDS) over SSL. This means developers can for the most part connect and interact with the database in the same fashion as within Microsoft SQL Server. Taking advantage of ADO.NET encryption and trusted server certificates is definitely worth considering, especially when accessing a SQL Azure database from through the

cloud. The connection properties Encrypt=True and TrustServerCertificate = False, in the proper combination, will help ensure that data transmission is secure and can help prevent man-in-the-middle attacks. This is also a requirement for connecting to SQL Azure—it is impossible to connect to SQL Azure unless connection-level encryption has been turned on.

By leveraging the encryption in transit features such as these, covered entities can enforce policies and procedures they deem necessary for HIPAA and ensure mechanisms implemented for encrypting sensitive data in transmission.

Identification and Authentication

Developers can leverage application layer Identification and Authentication controls through Windows Identity Foundation. This enables .NET developers to externalize identity logic from their application, improving developer productivity, enhancing application security, and enabling interoperability. Additionally, Microsoft offers:

- Active Directory Federation Services 2.0: a security token service for IT that issues and transforms claims and other tokens, manages user access and enables federation and access management for simplified single sign-on.
- Windows Azure Access Control Services: provides an easy way to provide identity and access control to web applications and services, while integrating with standards-based identity providers, including enterprise directories such as Active Directory®, and web identities such as Windows Live ID, Google, Yahoo! and Facebook.

These technologies enable covered entities and their business associates to satisfy Log-in monitoring, Password management, Unique User Identification, Automatic logoff, Person or entity authentication safeguard requirements within HIPAA.

Resources:

Windows Identity Foundation Simplifies User Access for Developers

Logging and Monitoring

Windows Azure Diagnostics allow collection of rich diagnostic data to assist in trouble shooting a deployed service. It provides support for a variety of diagnostic features including Windows Azure logs, Windows Event logs, IIS logs, Failed Request Tracing (commonly known as FREB) logs, application crash dumps, and performance counters, in addition to Windows Azure Diagnostic Monitor logs with data about the diagnostic feature itself. Windows Azure performs logging right out of the box—it's part of the Windows Azure SDK. There are some advantages to using a logging framework like Logger.NET, Enterprise Library, log4net or Ukadc.Diagnostics. These add additional structure to logging messages and also can help provide some of the configurability mentioned earlier.

Within SQL Azure, transaction logging is automatically managed by SQL Azure's infrastructure. SQL Server Analysis and Reporting Services are available and supported by SQL Azure, similar to the support within SQL Server 2008 R2. Additionally SQL Azure Reporting is a cloud-based

reporting service built on SQL Azure Database, SQL Server, and SQL Server Reporting Services technologies. It is possible to publish, view, and manage reports that display data from SQL Azure data sources.

These are representative safeguards that support compliance efforts allowing a covered entity to perform information system activity review, log-in monitoring, and ensure audit controls.

Resources:

Take Control of Logging and Tracing in Windows Azure

http://channel9.msdn.com/Learn/Courses/Azure/Deployment/DeployingApplicationsinWindowsAzure/Exercise-3-Monitoring-Applications-in-Windows-Azure

Patching SQL Azure

BUSINESS RESILIENCY

Business continuity

Business continuity risk, such as the management of backup and recovery facilities, can be transferred to by leveraging Microsoft cloud platforms. Microsoft can provide more robust and less expensive business continuity solutions than businesses can achieve alone.

CONTINUITY:

- Multiple geo based data centers
- Users can choose single location or geo-distributed data centers
- Storage data replicated multiple times
- Fabric is designed to be backed up and restored from checkpoints

Adopting Microsoft's cloud service means that Microsoft is responsible for disaster recovery. Microsoft treats disaster recovery seriously as an outage impacts our bottom line.

Easy geo-availability

Applications can take advantage of datacenter geo-distribution without high investment or development overhead. Microsoft's cloud services provide additional capacity on demand. Utilizing cloud bursting helps address unpredictable usage spikes as systems resume operations after disaster recovery. It also reduces the cost of disaster recovery infrastructure. Subscribers can replace parts of the dedicated disaster recovery infrastructure with reliance on Microsoft cloud infrastructure.

A financially backed SLA for Online Services

Our online services are designed to deliver reliability, availability, and performance with a guaranteed 99.9% uptime, financially backed service level agreement (SLA).

Microsoft is Your Trusted Data Steward

Our covered entity customers look to Microsoft as their trusted data steward, and have leveraged the robust array of safeguards that resulted in our ability to offer a Business Associate Agreement (BAA) as a standard operationalized component for a continually growing list of our cloud offerings. Microsoft's goal is to provide a unified and integrated platform that meets or exceeds the compliance requirements for healthcare covered entities.

EARNING YOUR TRUST – UNDERSTANDING THE PROBLEM SPACE

As a company that employs and self-insures more than 90,000 staff, Microsoft is in a unique position in which it must address compliance challenges such as HIPAA internally as well as through its products and services for its customers. Covered entities benefit from Microsoft's experience of addressing compliance challenges which can then be leveraged by product teams. Within Microsoft, we subscribe to a "eating your own dogfood" culture which puts us in the best position to understand the challenges face by our covered entity customers.

Microsoft's executives are your trusted advisors, with deep backgrounds in the Healthcare industry, and involvement in compliance.

ENABLING COMPLIANCE: EFFECTIVE & EFFICIENT PROCESS-DRIVEN FRAMEWORK

The Microsoft Compliance Framework for Online Services allows the company to better address complex obligations through reducing risk of operational disruptions and increasing confidence in service stability, and by obtaining third party verifications as proof of continuing adherence to compliance requirements.

Microsoft uses the control objectives given in ISO/IEC 27001:2005 as a starting point in an analysis of many other compliance requirements in order to create a superset of compliance control objectives that also accounts for HIPAA.

CONCLUSION

As trusted advisors to our customers and partners in health, Microsoft understands the importance of safeguarding electronic protected health information. As your trusted data steward, we share with you a common duty towards patients, and we ensure that our compliance supporting policies and procedures as a business associate are aligned with your own as a covered entity.

With that in mind, we maintain our commitment to support the healthcare industry with a paradigm shift in thinking about the role of IT. With our host of flexible cloud computing offerings across the spectrum of IaaS, PaaS, and SaaS, and their embedded security capabilities, we enable our customers and partners to realize tangible benefits such as cost reduction, business agility flexibility and scalability as well as compliance support for regulations including but not limited to HIPAA and HITECH.

We enable you to address the physical, technical, administrative and organizational safeguards required of covered entities using:

- Cloud infrastructure, platform and software offerings with embedded security and privacy controls
- A software development process that builds in on-going security
- Automated security policies in the operation of our datacenters
- Leading edge and constantly updated security technology embedded in our products
- Built-in business resiliency backed up by a money-back guarantee
- A process-driven framework for online security to support HIPAA requirements, but also through support of certifications such as ISO 27001, SAS 70 Type II, SSAE16, and EU Safe Harbor.

We are Microsoft in Health.

REFERENCES

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . Zaharia, M. (2009). *Above The Clouds: A Berkeley View of Cloud Computing*. Electrical Engineering and Computer Sciences. University of California at Berkeley. Retrieved from www.eecs.berkeley.edu/pubs/techrepts/2009/eecs-2009.html

Kanaan, S. B., & Carr, J. M. (2009). *Health Data Stewardship: What, Why, Who, How - An NCVHS Primer*. National Committee on Vital and Health Statistics.

APPENDIX A – MICROSOFT'S SECURITY DEVELOPMENT LIFECYCLE

Training Phase

Core Security Training

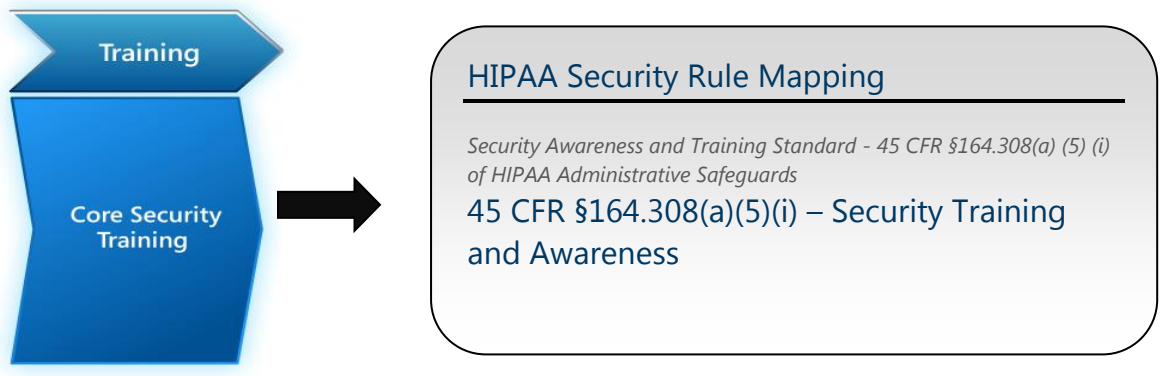


Figure 1-1: SDL Training Phase mapping to HIPAA Security Rule

The core security training that all Microsoft services staff adheres to, meets the HIPAA Security Rule Administrative Safeguard Standard for Security Awareness and Training.

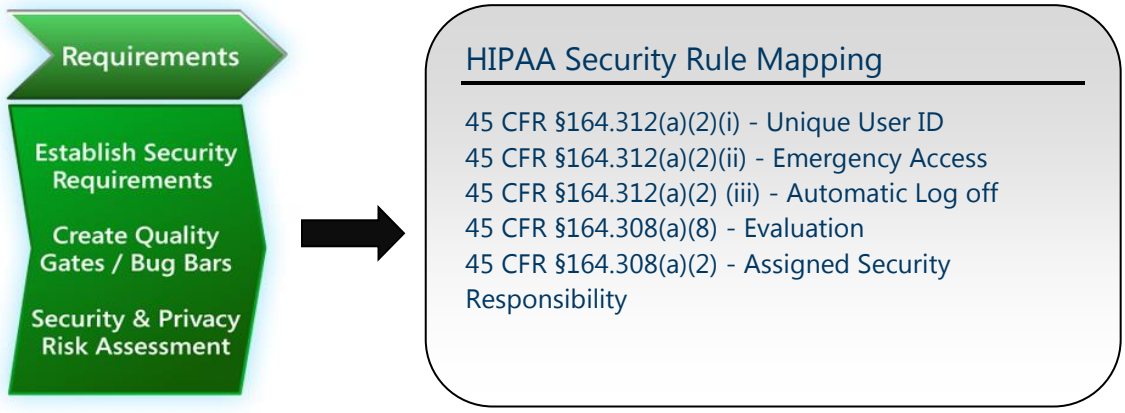
Each member of the Microsoft software development team receives appropriate training to stay abreast of security basics and recent trends in security and privacy. Members that serve technical roles must attend at least one unique security training class annually.

Basic software security training covers the following foundational concepts:

- Secure design
  - Attack surface reduction
  - Defense in depth
  - Principle of least privilege
  - Secure defaults
- Threat modeling
  - Overview of threat modeling
  - Design implications of a threat model
  - Coding constraints based on a threat model
- Secure coding
  - Buffer overruns (for applications using C and C++)
  - Integer arithmetic errors (for applications using C and C++)
  - Cross-site scripting (for managed code and web applications)
  - SQL injection (for managed code and web applications)
  - Weak cryptography
- Security testing
  - Differences between security testing and functional testing

    - Risk assessment
    - Security testing methods
- Privacy
    - Types of privacy-sensitive data
    - Privacy design best practices
    - Risk assessment
    - Privacy development best practices
    - Privacy testing best practices

Requirements Phase



- **Figure 1-2: SDL Requirements Phase mapping to HIPAA Security Rule**

Balancing the tradeoffs between feature functionality and security requirements is a key challenge commonly facing software development managers today. The Requirements Phase of the SDL discusses specifying the security and privacy requirements of the software to optimize integration of security and privacy during a project with feature functionality. It consists of three practices: Establishing Security and Privacy Requirements, Defining Quality Gates/Bug Bars, and Performing a Security and Privacy Risk Assessment. By specifying the security and privacy requirements of the software as part of a separate monitored process, we can ensure that development activities prioritize security and privacy appropriately and do not take a back seat to features. The HIPAA safeguards that align to the requirements phase of SDL demonstrate Microsoft's commitment to best practices commonly found throughout the Microsoft family of products and cloud services.

Establish Security Requirements

Security requirements are gathered at the early stages of software development to ensure secure system development. Through establishing security requirements in the initial stages of software development, Microsoft teams identify key security and privacy concerns for their

products early on in the development life cycle. Some of the security and privacy requirements analysis in this phase includes:

- Assigning security experts
- Defining minimum security and privacy criteria for the application as designed to run in its planned operational environment.
- Specifying and deploying a security vulnerability/work item tracking system that allows for creation, triage, assignment, tracking, remediation, and reporting of software vulnerabilities

Define Quality Gates/Bug Bars

Microsoft teams use quality gates and bug bars to define and establish minimum acceptable levels of security and privacy quality as part of their software development lifecycle. Bug bars are quality gates that apply to the entire software development project and define the severity thresholds of security vulnerabilities. They allow for the identification and implementation of technical safeguards early on in the development process. Upon the successful implementation of the safeguards, the product team must demonstrate compliance and undergo a Final Security Review before the product is made available. A formal documented exception "quality gates and bugs" process is also defined in this phase of the security development process.

Perform Security and Privacy Risk Assessment

Security and Privacy Risk Assessments are performed in the Requirements phase to identify functional aspects of the software that require closer reviews. Risk assessments help management understand the cost and requirements involved in handling data governed by security and privacy considerations for information containing Electronic Protected Health Information (ePHI). Security Risk Assessments conducted by Microsoft product teams include analyzing source code, authentication mechanisms, authorization practices, cryptography, file access controls, networking and messaging capabilities, services accounts and privileges, and database or web services. Privacy Risk Assessments assign an impact rating based on the following guidelines:

- P1 High Privacy Risk: The feature, product, or service stores or transfers PII or PHI, changes settings or file type associations, or installs software.
- P2 Moderate Privacy Risk: The sole behavior that affects privacy in the feature, product, or service is a one-time, user-initiated, anonymous data transfer (for example, the user clicks on a link and the software goes out to a web site).
- P3 Low Privacy Risk: No behaviors exist within the feature, product, or service that affects privacy. No anonymous or personal data is transferred, no PII or PHI is stored on the machine, no settings are changed on the user's behalf, and no software is installed.

Design Phase

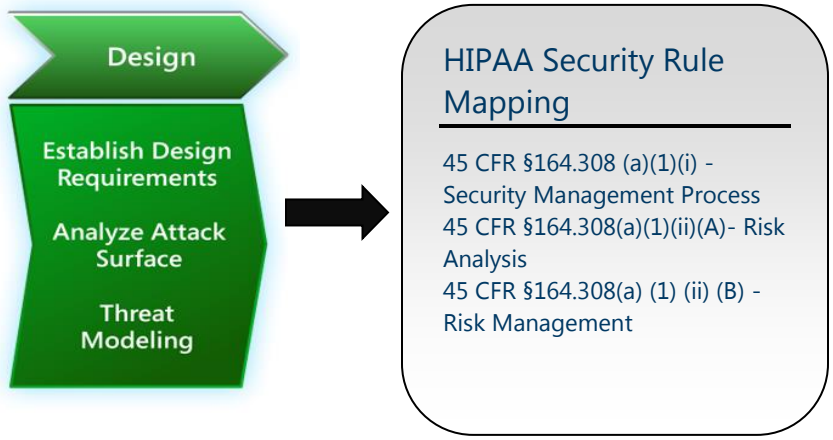


Figure 1-3: SDL Design Phase mapping to HIPAA Security Rule

In the Design Phase of the SDL process, the security architecture of the software is defined and documented. The actions involved in defining the design requirements include the creation of security and privacy specifications based on the requirements, a specification review, and the specification of minimum cryptographic design requirements. A key best practice in the design phase entails the data awareness of various information types in that you can only apply the appropriate safeguards when you understand your dataset and your data flow. The design specification of privacy and security requirements details the potential exposure factors of personal health information therefore ensuring that software features do not compromise security.

Establish Design Requirements

When establishing design requirements, Microsoft product teams create security and privacy design controls, and employ cryptographic mechanisms as necessary to meet HIPAA security rule safeguards. Below is a list of the cryptographic algorithms approved by the SDL. The list of SDL-approved algorithms is reviewed and updated annually as part of the SDL update process.

- Use AES for symmetric encryption /decryption with 128-bit or better symmetric keys.
- Use RSA for asymmetric encryption /decryption and signatures with 2048-bit or better RSA keys.
- Use SHA-256 or better for hashing and message-authentication codes.

Attack Surface Analysis /Reduction

When an oncologist assesses risks associated with skin cancer, he or she will assess your skin complexion, your sun exposure, and your use of sunblock. Just as in assessing skin cancer risk, attack surface analysis can identify potential exposures that can threaten your application's integrity or data. Attack surface reduction is a means of reducing risk by giving attackers less opportunity to exploit a potential weak spot or vulnerability. This helps the development team to reduce and thwart threats to the attack surface by limiting, disabling, or restricting access to

system services, applying least privilege controls, and employing layered defense mechanisms in Microsoft products.

Threat Modeling

Microsoft product teams use threat modeling to understand the security threats to a system, determine risks from identified threats, and establish appropriate mitigations. The threat modeling process is a systematic approach for software developers to identify threats and vulnerabilities to software prior to software release. This process is practiced by Microsoft products teams in new releases and update releases.

Verification Phase

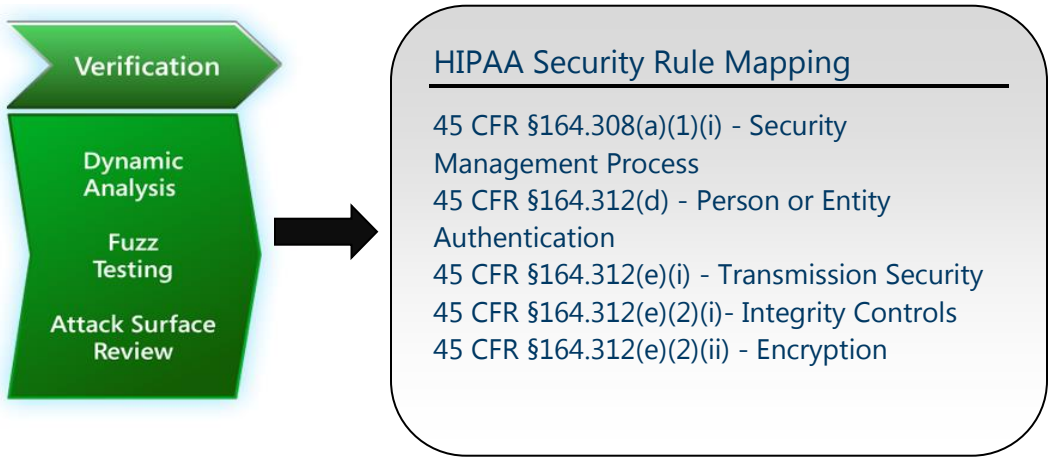


Figure 1-4: SDL Verification Phase mapping to HIPAA Security Rule

The verification phase is the phase in which security testing occurs. During this phase, the security and privacy requirements specified in the earlier stages of software development are evaluated in three different sub phases: Performing Dynamic Analysis, Fuzz Testing, and Attack Surface Review.

Perform Dynamics Analysis

Dynamic analysis is run-time verification of the software programs to ensure that the software functionality works as designed. Dynamic analysis is done by leveraging tools that monitor application behavior for memory corruption, user privilege issues, and other critical security problems. Microsoft cloud product teams utilize a host of run-time tools to ensure accurate and complete security testing of the completed software product.

Fuzz Testing

Part of the verification phase includes fuzz testing of the application. Fuzz testing is a specialized form of dynamic analysis that induces program failure by deliberately introducing malformed or random data into the application.

Attack Surface Review

The last sub phase of the verification phase is a comprehensive review that complements the Attack Surface Analysis/Reduction carried out in the Design phase focusing on the design and implementation deviations from design and functional specifications in the Design phase. Such deviations are analyzed for potential new threats or attack vectors and additional threat modeling is conducted in this sub phase to ensure that risks stemming from design specifications deviations are mitigated.