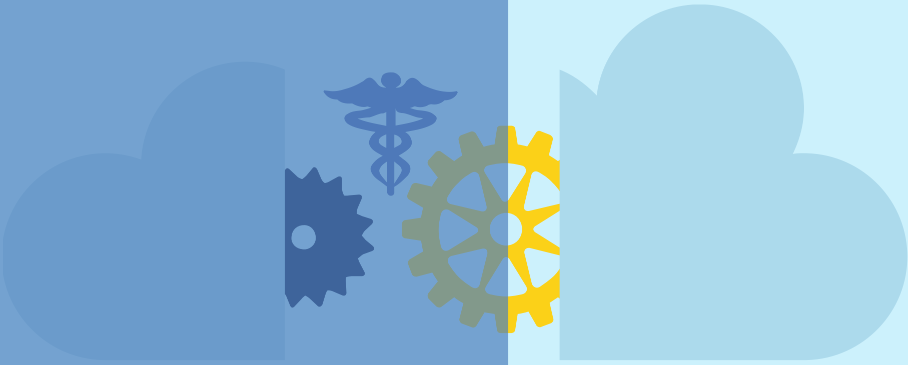


A Practical Guide to

DESIGNING SECURE HEALTH SOLUTIONS

Using Microsoft Azure

Executive Overview

Since its launch in 2010, Microsoft® Azure™ has gained rapid adoption from organizations of all sizes around the world, spanning many industries. The users of Azure benefit from agility, reduced costs and complexity, limitless scale, and innovation made possible by cloud computing.

For organizations in regulated industries, such as healthcare, where laws regulate protected health information (PHI), the need to understand how cloud adoption affects their privacy, security, and regulatory compliance posture is paramount. These organizations should seek deeper understanding and guidance in solution design and cloud deployment operations.

Disclaimer

Published August 2015

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

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

NOTE: Certain recommendations in this paper may result in increased data, network, or compute resource usage, and may increase your license or subscription costs.

Acknowledgements

Authors: Marc Kuperstein, Frank Simorjay, Leslie Sistla

Contributors: David Cross, Kurt Dillard, Alison Howard (LCA), Katie Look, Tom Shinder, Joel Sloss

Reviewers: Yuri Diogenes, Terry Lanfear, Steven Powell, Tom Quinn

Table of Contents

Intended audience

This paper will be most helpful to those in regulated industries who need guidance and best practices in designing secure solutions on Azure:

- Chief Information Security Officers (CISOs), Chief Risk Officers (CROs), Chief Privacy Officers (CPOs), Chief Compliance Officers (CCOs), IT professionals, and security specialists. Also, anyone who wants to understand how compliance obligations are met on Azure.

- Solution architects, developers, and operations staff. The paper will be useful to individuals who are already familiar with how Azure functions from a broad perspective, and who want to understand how to apply security principles in designing and operating cloud solutions that are aligned with compliance considerations in solution design.

As a starting point for intended audiences, refer to the Azure HIPAA Implementation Guidance. This document was developed to assist customers who are interested in Health Insurance Portability and Accountability Act of 1996 and (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) to understand the relevant capabilities of Azure.

For additional information and security guidance, please refer to the following sites:

Privacy, Security and Compliance Resources on Azure Trust Center
AzureCAT Guidance – application design patterns
Azure.com | Documentation | Best Practices – checklists
Azure.com/Documentation Center – service documentation

Introduction

Health industry startups, system integrators (SIs), independent software vendors (ISVs), and healthcare organizations considering a move to Azure are looking for guidance in designing and operating solutions that incorporate security controls to help them meet their compliance obligations.

Azure provides services that can help meet the security, privacy, and compliance needs of Microsoft customers. In addition, Microsoft works with customers to help them understand their responsibilities to protect their data and environment infrastructure after their service has been provisioned. This infrastructure includes applications, data content, virtual machines, access credentials, and compliance issues requirements.

This Microsoft guidance helps customers understand how they can improve security of their solution service simply and effectively. In addition, each customer should have their own compliance mechanisms, policies, and procedures in place to ensure they do not use Azure in a way that violates any regulatory requirements. Users of Azure should independently verify with their own legal counsel that their implementation meets all local compliance regulatory requirements.

This paper provides insight into how Microsoft meets its compliance obligations on the platform and presents best practices and security principles that are aligned to International Organization for Standardization (ISO) 27001, Microsoft's Security Development Lifecycle (SDL), and operational security for Microsoft online services.

The content is divided into three major sections:

1. Considerations guidance for using cloud technology, includes risk management, shared responsibility considerations, establishing an information security management system, understanding industry and local regulations, and establishing standard operating procedures.

Primary Audience: CISOs/Risk managers | Secondary Audience: Solution architects/Developers

2. Key security principles that are both aligned to a standard information security management standard, such as ISO 27001, and standard development processes, such as Microsoft's Security Development Lifecycle (SDL).

Primary Audience: Solution architects/Developers/Operations | Secondary Audience: CISOs/Risk managers

3. Applying the key principles to use cases by demonstrating alignment from a solution architect perspective, where requirements for the solutions are aligned to the information security management standard.

Primary Audience: Solution architects/Developers/Operations | Secondary Audience: CISOs/Risk managers

Compliance and security methodology

This guidance is rooted in well-established standards such as those from ISO, the National Institute of Standards and Technology (NIST), and Health Level-7 (HL7) based as a foundation for establishing an information security management system (ISMS). After such a system is set and the key ISMS best practices are established, the focus incorporates three key areas:

- Health industry compliance considerations
- Adopting secure development processes
- Establishing secure operations principles

The intention is to ensure that standard security development and operations best practices are incorporated from the beginning of a cloud project, and key activities are communicated effectively with all the stakeholders in the context appropriate for their roles. These roles include: compliance officers, legal advisors, risk managers, solution architects, developers, and operations personnel.

Best practices and recommendations will be presented in the subsequent sections. The following list specifies the sections and their alignment to the standards ISO, NIST, and HL7:

Foundation

- Establishing an ISMS | Aligned to ISO 27001
- Establishing standard operating procedures that align to the ISMS | Aligned to ISO 27001

Compliance considerations

- Compliance regulations such as HIPAA and EU DPD (European Union Data Protection Directive) with clearly defined physical, technical, and administrative safeguards | Aligned to ISO 27001

Tools for solution design

- Adopt data governance practices | Aligned to ISO 27001 or HL7
- Security Development Lifecycle | Aligned to ISO 27001
- Operational security for Microsoft online services | Aligned to ISO 27001 and NIST
- 13 key security principles for designing and securing solutions for Azure are presented, with recommendations | Aligned to ISO 27001

Use cases – principles applied in an industry-focused scenario

Aligning using ISO

Initially, organizations should consider adopting an information security management system. One example is ISO 27001, an auditable, international, information security management standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that formally defines requirements for a complete ISMS to help protect and secure an organization's data. ISO 27001 details a set of best practices and is intended to be applicable to all organizations, regardless of their type or size.

For organizations that deal with sensitive information, the ratified ISO 27018, an extension of the ISO 27001 standard, governs the processing of personally identifiable information (PII) by cloud service providers acting as

PII processors. ISO 27018 details controls that address protecting PII in public cloud services. Azure was the first global cloud service to adopt ISO 27018, which provides an additional set of controls for an organization to consider when adopting an ISMS.

ISO 27002 is a complementary collection of 114 controls and best practice guidelines designed to meet the requirements detailed within ISO 27001. The controls are organized into 14 groups, and when properly implemented can help an organization achieve and maintain information security compliance by addressing specific issues that are identified during formal, periodic risk assessments. These 14 groups are:

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition
- Development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management

Establishing or re-invigorating an ISMS is a very deep and broad topic with complex challenges, and there are many resources available to assist organizations in this endeavor. Organizations should consider conducting a risk assessment and aligning risk management and mitigation to that assessment. A second area of focus that organizations should consider is establishing standard operating procedures for each of the 14 ISO groups to establish core principles for the entire organization to follow.

Risk management

One of the best practices defined in ISO 27001 is on risk assessment and risk management. Organizations, especially those in regulated industries, are advised to undertake an assessment and manage for risks.

There are no shortages of risk management approaches, and organizations can adopt one that is appropriate for their needs. One approach could involve ISO 31000, which is focused specifically on risk management. In the US healthcare industry, the HIPAA statute requires a risk assessment and recommends the NIST Special Publication 800-30. Another approach could involve a portion of the NIST Special Publication 800-53 (FedRAMP). Within it, a risk management framework is presented with specific activities. For a specific industry and locale, there may be a standard approach that is well-suited to assess and mitigate risks. Understanding risks is key to helping organizations choose the right controls.

Standard operating procedures (SOP)

Organizations should consider establishing SOPs around critical areas of their ISMS. One way is to establish SOPs that align to each ISO group, identifying an accountable owner who will maintain and operate within an organization. The following examples are presented with some guidelines for:

Privacy

ISVs, especially those that are developing and deploying software as a service (SaaS) solutions for their customers, will have to consider the implication of handling data on behalf of their customers. They should consider providing a formal privacy statement that aligns with their internal processes and practices and that meets the commitments Details about Azure privacy commitments can be found at Microsoft Online Services Privacy Statement.

Incident response management

An important element that all organizations should implement is an organizational incident response plan. An incident response should consider the following four areas:

- Preparation. Assemble a core team of experts that will be available to respond to incidents. This team must be provided with response training, to be ready to respond quickly and effectively when a security incident occurs.
- Define a response plan. A plan that includes initial assessment, communication containment methods, and notification must be created. This plan must be kept current and up-to-date.
- Recovery. Part of the response plan should provide staff with the ability to bring systems back into working state. This step often includes suggestions and recommendations for additional monitoring and penetration testing to validate mitigation efficacy.
- Lessons learned. After resolution of the security incident, the response team should evaluate the event and record lessons learned during the incident response process.

For more detailed information about an incident response plan, see the Responding to IT security Incidents article.

When establishing a standard ISMS within an organization, the need to align and adopt well-known and refined standard practices cannot be overemphasized.

ISO27001, 27002, and 27018 are standard practices to help protect IT environments from threats. These standards can help to design a robust secure environment and move it toward a state of compliance for demonstration to regulators. Meeting these obligations will achieve a high quality bar for the industry, health in this case. This process is well defined and provides a set of basic guidelines that can be followed for successful adoption of Azure-based solutions.

Incorporating regulation considerations – health industry

Health regulations differ between countries/regions and some times even between states. An understanding of these regulations requires careful legal analysis to determine and establish which controls are necessary to demonstrate compliance with local laws.

From a platform perspective, Azure meets a broad set of international and industry-specific compliance standards and regulations applicable to cloud service providers, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards including Australia IRAP, UK G-Cloud, and Singapore MTCS. Details of all compliance programs can be found on the Microsoft Azure Trust Center.

There is no third-party certification for HIPAA or the EU Data Protection Directive. The ISO 27001 audit scope includes controls that address HIPAA security practices as recommended by the US Department of Health and Human Services and the EU Data Protection Directive. This is a key reason why ISO 27001 is the basis for the guidance in this paper.

A few more details about these two regulations are provided in the following paragraphs:

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a United States law that applies to "covered entities" – doctors' offices, hospitals, health insurers, and other healthcare entities with access to patients' protected health information, or PHI.

The law regulates the dissemination of PHI and is organized into four general areas:

- Privacy covers patient confidentiality.
- Security deals with the safety of information, including physical, technological, and administrative safety.
- Identifiers specify the types of information that cannot be released if information is collected for research purposes.
- Codes for electronic transmission of data in healthcare-related transactions, including payments, insurance claims, eligibility, referrals, enrollments, and authorizations.

The scope and depth of HIPAA were extended in 2009 with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Together, HIPAA and HITECH put forth strict standards that govern information security and privacy for PHI.

The Azure HIPAA Implementation Guidance provides core information to assist customers who are interested in HIPAA and the HITECH Act to understand the relevant capabilities of Azure.

EU Data Protection Directive

Although the EU Data Protection Directive 95/46/EC is not healthcare-specific, it is a comprehensive privacy standard for processing persona data from member states in the EU. Article 8 of the EU Data Protection Directive 95/46/EC makes provisions for "the processing of special categories of data" including personal data concerning health. Each member state may choose to add additional controls based on this provision for sensitive health data. Some member states have not added any controls specific to health care, thus making cloud adoption with EU Model Clauses possible without additional regulatory barriers in those member countries.

The EU Model Clauses are standardized contractual clauses used in agreements between service providers (such as Microsoft when it offers Azure services under the EU Model Clauses) and their customers to ensure, in a standardized way, that the appropriate safeguards are in place to protect personal data that leaves the European Economic Area (EEA).

Compliance with EU data protection laws also means that on a practical level customers need fewer approvals from individual data protection authorities to transfer personal data outside of the EU. The reason for this is because most EU Member States do not require an additional prior authorization from the local data protection authority if the transfer is based on an agreement that complies with the Model Clauses.

Microsoft was the first company to receive a letter of endorsement and joint approval from the EU's Article 29 Working Party, which includes data protection authorities from each of the EU member states, for its strong contractual commitments to comply with EU data protection laws regarding the international transfer of data. Azure agreements include the EU Model Clauses that provide customers additional guarantees around transfers of personal data for the Azure services that are in-scope. This inclusion ensures that customers can use Microsoft cloud services to move data freely through the Microsoft cloud from Europe to the rest of the world.

Not all services are covered by the contractual agreements upon services' general availability. The services must achieve the ISO 27001 certification first, and may then be added to an in-scope service list. In-scope Azure services can be found here for the HIPAA Business Associate Agreement (BAA) and the EU Model Clauses. These services are independently audited once a year for ISO 27001/27002 and 27018 compliance by British Standards Institution (BSI) Americas, an ISO accredited auditor. The current compliance certificate may be found here.

On Azure, both these contractual agreements are incorporated in the Online Services Terms (OST); execution of the volume licensing agreement includes execution of EU Model Clauses and, for applicable customers, the BAA, unless the customer opts out.

Considerations and tools for success

After an ISMS foundation is set and best practices are adopted, additional areas need to be evaluated and understood to determine an organization's risk posture and keys for mitigating its risks.

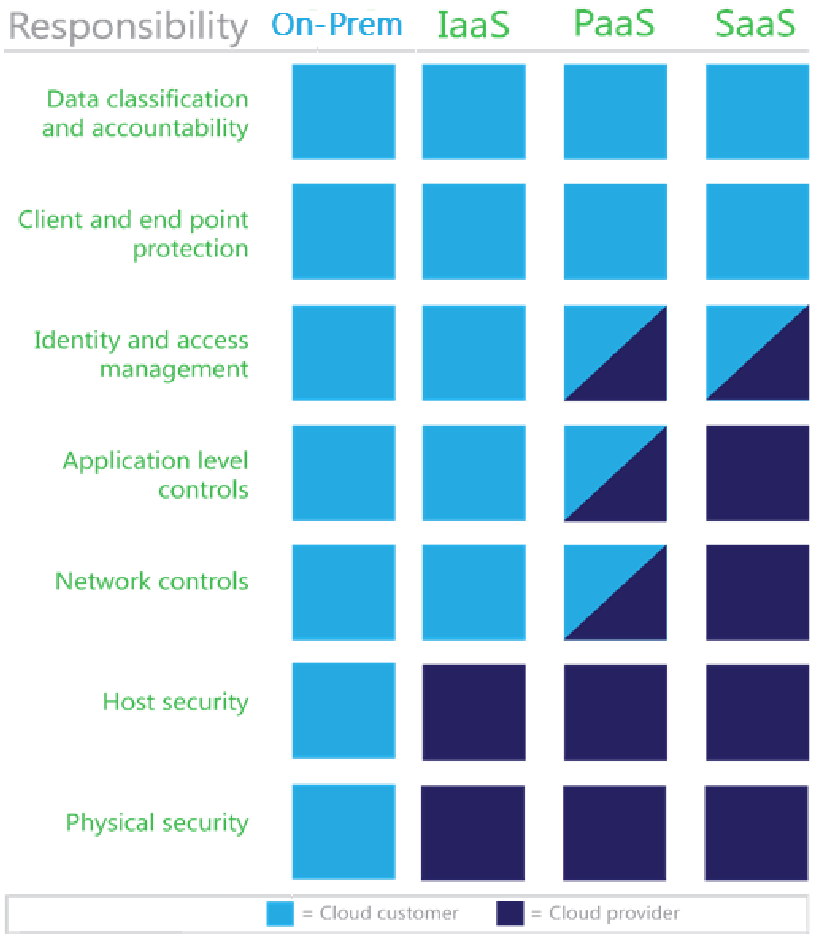
The first area is understanding the principles of shared responsibilities for meeting compliance, where customers and the cloud provider have distinct responsibilities in meeting compliance end to end. Organizations need to understand what service models are being used in the design and then determine what controls need to be in place to meet their compliance needs. Organizations also need to understand which areas the cloud provider is responsible for with regard to meeting compliance obligations, and which areas are the responsibility of the user or organization.

Another consideration is establishing governance practices, that include the practice of classifying data and protecting it based on different levels of data sensitivities.

Incorporating both these considerations in a solution design will help present a clear picture of how to mitigate for risks and design with compliance in mind.

Shared responsibilities

The widely understood cloud service models as defined in the NIST Definition of Cloud Computing, Special Publication 800-145 are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The service model that is chosen by customers also dictates the responsibilities of managing their cloud environment. The following diagram shows the split in responsibilities by key areas and is critical for all customers to understand, but especially those in regulated industries as they assess and mitigate risks.



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability	🟦	🟦	🟦	🟦
Client and end point protection	🟦	🟦	🟦	🟦
Identity and access management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	⬛
Network controls	🟦	🟦	◩	⬛
Host security	🟦	⬛	⬛	⬛
Physical security	🟦	⬛	⬛	⬛

🟦 = Cloud customer ⬛ = Cloud provider

- The customer is completely responsible for all aspects of operations when solutions are deployed on-premises.
- With IaaS, the lower levels of the stack, physical hosts or servers, and host security are managed by the platform vendor. The customer is still responsible for securing and managing the operating system, network configuration, applications, identity, clients, and data. For the developer, an obvious benefit with IaaS is that it reduces the developer requirement in configuring physical computers.
- With PaaS, everything from network connectivity through the runtime or identity service may be provided and managed by the platform vendor. PaaS offerings further reduce the developer burden by additionally supporting the platform runtime and related application services. With PaaS, the developer can almost immediately begin creating the business logic for an application.
- With SaaS, a vendor provides the application and abstracts customers from all of the underlying components. Nonetheless, the customer continues to be responsible to ensure that data is classified correctly and that user devices are secured and protected when connected to the service.

Applying data governance practices

Organizations need to be able to make decisions about how to:

- Manage data
- Realize value from data
- Minimize cost and complexity
- Manage risk
- Ensure compliance with ever-evolving legal, regulatory, and other business requirements

An important part of data governance practice is a quality control effort program for assessing, managing, and protecting information. It is a way of assigning the responsibility, authority, and accountability for information-related processes, executed according to organization-designed models. It also describes who can take what actions with which information, when action can occur, under what circumstances, and with which methods. Such a program:

- Serves as the channel where key decisions about information management are communicated.
- Acts as a vehicle to ensure compliance and establish accountability around defined data policies and standards.
- Involves data owners and data stewards who have a broad understanding of the data required for a set of business processes.
- Develops, institutionalizes, and socializes policy, data standards, and information management processes.

Objectives for a successful program include:

- Improve decision making of the management team.
- Ensure data consistency.
- Build trust of data among everyone involved in the process.
- Adhere to compliance requirements.
- Eliminate risks related to data.

When data is responsibly classified and managed, organizations can grant access to use and purpose the data while also taking full advantage of enabling technologies and safeguarding sensitive content. Data governance provides a viable approach to enabling a dynamic environment that is capable of quickly adapting to innovation, transformation, and other efficiencies.

Healthcare standard developing organizations (SDOs) such as HL7 have issued implementation guidance on Healthcare Privacy and Security Classification System (HCS) as a way to automate labeling and segmentation of protected healthcare information by access control systems to enforce privacy and security policies.

As a general starting point, Microsoft's Protect and control your key information assets through information classification white paper and framework, which is available for download. This document discusses information classification as the foundation of the cross-organization effort, the suggested approach to sustain such an effort and thus to handle and manage information assets on that basis, as well as the Microsoft services, products, and technologies to consider in this context to implement a relevant information classification and enforcement infrastructure. It constitutes the starting point for an effective information protection and control (IPC) system.

Applying security practices

In addition to sound information security management practices, Microsoft makes security and privacy a priority at every step in producing and managing software for both cloud and on-premises users of software and services around the world. Supporting that commitment, the Microsoft Security Development Lifecycle (SDL) and Microsoft operational security for online services are adopted across the company. Organizations adopting similar standard practices can help mitigate security risks.

- The Security Development Lifecycle (SDL) is a security assurance process that is focused on software development. As a company-wide initiative and a mandatory policy across Microsoft since 2004, the SDL has played a critical role in embedding security and privacy in software and culture at Microsoft. Combining a holistic and practical approach, the SDL aims to reduce the number and severity of vulnerabilities in software. The SDL introduces security and privacy throughout all phases of the development process. In 2011, the Microsoft Security Development Lifecycle (SDL)SDL was deemed by the ISO to meet or exceed the guidance published in ISO 27034-1.

  ISO 27034 provides guidance for a risk-based and continuously improving software security management system applied across the application lifecycle. ISO/ 27034-1, Annex A contains a case study that illustrates how the SDL conforms to the components and processes of ISO 27034. ISO 27034-1 is published on the ISO website.

- The Microsoft operational security for online services white paper addresses operational security needs in a way that takes advantage of SDL knowledge and processes. Operational security for Microsoft online services is a framework that focuses on infrastructure issues to help ensure secure operations throughout the lifecycle of cloud-based services. The following list includes a number of ways that illustrates how operational security for Microsoft online services adds considerable value to the focus on infrastructure issues and operational security:
  - Use of a proven methodology for verification and continuous improvement that was first established with the SDL and is closely tied to Microsoft Security Response Center (MSRC) incident response processes.
  - Support for Microsoft internal security policies that align with standards such as NIST 800-53, ISO 27001, and other related industry guidance that applies to a broad range of cloud services. It also reflects Microsoft experience in the secure operation of online services.
  - Protection against Internet-based external threats.
    - Operational security for online services is designed to better discover attacks as a way to inform future security improvements.
    - Operational security for online services prescribes key security controls that Microsoft has seen to be effective in mitigating known attacks and previously unknown vulnerabilities.
    - Takes advantage of decades of Microsoft experience operating cloud services at scale.
    - Integration with the SDL, so that changes in operations can result in changes to the development of software used in operations and vice-versa. More importantly, operational security for Microsoft online services creates a feedback cycle that Microsoft can use to update its operational processes more rapidly than a typical policy cadence can support.
  - Repeatable practices and methodology that are used to actively and continuously update services to improve security and resolve incidents as quickly as possible.

The Mapping process

The following chart illustrates a way to map controls, processes, and compliance safeguards to help align secure development and operations with compliance obligations. This mapping should not be considered inclusive of all compliance requirements nor presented in the depth necessary for a specific organization's needs, but is offered as best practice guidance, an approach that uses well-known standards as the foundation.

- The first column presents the ISO 27001 group – the foundation.
- The second column presents the key security principle (detailed in the following section). It is a specific control within that ISO group, and is meaningful in developing secure software and/or operationalizing software.
- The third column presents whether that domain aligns with the SDL.
- The fourth column presents whether that domain aligns with operational security for Microsoft online services.
- The fifth column presents HIPAA safeguards. NOTE: This is neither complete nor offered as a checklist – it's the approach.
- The sixth column presents EU DPD safeguards. NOTE: Only a high level check indicates the compliance program applies – detailed control is in the EU Data Protection Directive.

				Compliance Programs	
ISO Groups	Key Security Principles (section to follow)	SDL	OSMOS	HIPAA	EU DPD
Information security policies		✓	✓	✓	✓
Organization of information security		✓	✓	✓	✓
	(1) Enable Identity and Authentication solutions			45 CFR §164.308 (a)(3)(i) 45 CFR §164.312 (a)(1) 45 CFR §164.312 (a)(2)(ii) 45 CFR §164.308 (a)(4)(ii)(B) 45 CFR §164.308 (a)(4)(ii)(C)	
Human resource security					
Asset management			✓	✓	✓
	(1) Enable Identity and Authentication solutions			45 CFR §164.308 (a)(3)(i) 45 CFR §164.312 (a)(1) 45 CFR §164.312 (a)(2)(ii) 45 CFR §164.308 (a)(4)(ii)(B) 45 CFR §164.308 (a)(4)(ii)(C)	
Access control		✓	✓	✓	✓
	(2) Use appropriate Access Control			45 CFR §164.308 (a)(1)(ii)(D) 45 CFR §164.308 (a)(3)(ii)(A) 45 CFR §164.308 (a)(4)(ii)(A) 45 CFR §164.308 (a)(5)(ii)(C) 45 CFR §164.308 (a)(3)(ii)(C) 45 CFR §164.308 (a)(5)(ii)(D) 45 CFR §164.312 (a)(2)(i) 45 CFR §164.312 (a)(2)(iii) 45 CFR §164.312 (d) 45 CFR §164.312 (b)	
Cryptography		✓		✓	✓
	(5) Encrypt all your customer data			45 CFR §164.312 (e)(1)(2)(ii) 45 CFR §164.308 (a)(5)(ii)(D) 45 CFR §164.312 (e)(1) 45 CFR §164.312 (e)(2)(ii)	
Physical and environmental security			✓	✓	✓
	(10) Train all staff in cyber security			45 CFR §164.308 (a)(5)(i) 45 CFR §164.308 (a)(5)(ii)(A)	
Operational security			✓	✓	✓
	(12) Keep you service and server Inventory current and up to date			45 CFR §164.308 (a)(1)(ii)(A) 45 CFR §164.308 (a)(8)	
Communications security					

				Compliance Programs	
ISO Groups	Key Security Principles (section to follow)	SDL	OSMOS	HIPAA	EU DPD
System acquisition, development and maintenance		✓	✓	✓	✓
	(4) Effective Certificates Acquisition and Management				
	(5) Encrypt all your customer data			45 CFR §164.312 (e)(1)(2)(ii) 45 CFR §164.308 (a)(5)(ii)(D) 45 CFR §164.312 (e)(1) 45 CFR §164.312 (e)(2)(ii)	
Supplier relationships				✓	✓
	(2) Use appropriate Access Control			45 CFR §164.308 (a)(1)(ii)(D) 45 CFR §164.308 (a)(3)(ii)(A) 45 CFR §164.308 (a)(4)(ii)(A) 45 CFR §164.308 (a)(5)(ii)(C) 45 CFR §164.308 (a)(3)(ii)(C) 45 CFR §164.308 (a)(5)(ii)(D) 45 CFR §164.312 (a)(2)(i) 45 CFR §164.312 (a)(2)(iii) 45 CFR §164.312 (d) 45 CFR §164.312 (b)	
Information security incident management		✓	✓	✓	✓
	(3) Use Industry recommended enterprise wide Anti-Malware solution			45 CFR §164.308 (a)(5)(ii)(B)	
	(8) Log security events, implement monitoring, visualization capabilities			45 CFR §164.308 (a)(1)(ii)(D) 45 CFR §164.312 (b) 45 CFR §164.308 (a)(5)(ii)	
	(11) Patch all systems and ensure security update are deployed			45 CFR §164.308 (a)(1)(i)(ii)(A) 45 CFR §164.308 (a)(1)(i)(ii)(B) 45 CFR §164.308 (a)(5)(i)(ii)(B)	
Information security aspects of business continuity management		✓		✓	✓
	(9) Determine the root cause of your incidents			45 CFR §164.308 (a)(7)(ii)(D)	
Compliance			✓	✓	✓
	(5) Encrypt all your customer data			45 CFR §164.312 (e)(1)(2)(ii) 45 CFR §164.308 (a)(5)(ii)(D) 45 CFR §164.312 (e)(1) 45 CFR §164.312 (e)(2)(ii)	
	(6) Penetration testing				
	(7) Threat Modeling services and application			45 CFR §164.308 (a)(1)(i) 45 CFR §164.312 (d) 45 CFR §164.312 (e)(i) 45 CFR §164.312 (e)(2)(i)	
	(11) Patch all systems and ensure security update are deployed			45 CFR §164.308 (a)(1)(i)(ii)(A) 45 CFR §164.308 (a)(1)(i)(ii)(B) 45 CFR §164.308 (a)(5)(i)(ii)(B)	
	(13) Maintain clear server configuration with security in mind			45 CFR §164.308 (a)(5)(ii)(C) 45 CFR §164.312 (b)	

Key principles and recommendations for secure development and operations

The following key security principles align with ISO 27001 controls. Of the 14 ISO 27001 groups and 114 controls, these 13 key principles have the most relevance to secure development and operations and so are highlighted with recommendations.

These security principles are designed to make cloud-based solutions more resilient to attack by decreasing the amount of time needed to prevent, detect, contain, and respond to real and potential Internet-based security threats, thereby increasing the security of related services.

By incorporating these principles and recommendations, customers can help mitigate and manage security risks from early stages of their adoption of cloud computing.

1. Enable identity and authentication solutions

Identity and authentication are essential to implement SDL effectively and securely. The implementation of these capabilities is important for identifying unique users of a service because they help ensure that only the right person accesses the service. The correct implementation will help ensure that the user who is logging in is actually the user that was assigned access rights.

Identity management remains a priority, even as business networks change. Identity management is as much about preventing unauthorized access to data as it is about controlling the authorized use of data. Identity management helps systems control the amount and type of data that users can access. A well-implemented solution helps ensure that users who are performing necessary functions are doing so at the appropriate privilege level. Identity management is also critical for maintaining separation of roles and duties, which may be required by specific regulatory and compliance standards. Knowing who a user is lets an application determine how it should interact with that user. Managing identity is just as important in the public cloud as it is in on-premises environments.

Azure provides services to help track identity as well as integrate it with identity stores that may already be in use. Azure Active Directory (Azure AD) is a comprehensive identity and access management service for the cloud that helps secure access to data in on-premises and cloud applications; it also simplifies the management of users and groups. It combines core directory services, advanced identity governance, security, and application access management.

Azure AD provides developers an effective way to integrate identity management in their applications. Identity and authentication are the first line of security defense at the organizational level and have the potential to be the weakest link in the security chain because they are the primary control that opens the 'door' to access management on which many aspects of security rely.

Recommendations:

- Identities should be kept up-to-date and managed for changes, additions, and removals. Ensure that only qualified individuals are made administrators. In addition, consider creating a unique user group to manage and log identities. Store customer identities in custom repositories such as Azure Active Directory.

- Connections between services should be implemented through a virtual private network, such as Virtual Network Configuration, which can provide site-to-site or point-to-site encryption. Additional services such as ExpressRoute can also be implemented.
- Grant appropriate access to Azure AD users, groups, and services by assigning roles to them using Azure AD role-based access control (RBAC).
- Because a compromised user account with privileged access (admin access) could affect overall cloud security, lessen risks by monitoring admins using Azure AD Privileged Identity Management. Manage the identities of portal administrators by adding or removing permanent or temporary administrators to each role using Privileged Role Management.
- Enable on-demand, "just in time" administrative access to directory resources.
- Ensure that permissions to sensitive data follow the least privilege principle and grant access for only the minimum necessary time needed for each role.
- Understand the core architecture of cloud identity by reading the Azure Identity Fundamentals article.

As with identity, authentication is essential for managing user identities. Authentication is the process of proving identity, typically through credentials, such as a user name and password. A growing number of employees, partners, and vendors require access from outside the office walls. And because of the bring your own device (BYOD) movement, that access is no longer limited to company-owned and managed laptops.

Users often connect from personal and mobile devices across unsecured networks. Organizational data and applications are on the move over these networks. With escalating IT security threats and a growing number of users, applications, and devices, multi-factor authentication has become the new standard for securing access.

Recommendations:

- Enable multi-factor authentication functionality for both cloud and on-premises applications.
- Establish strong password policies to manage user accounts stored in Azure AD. It is important that passwords and secrets be securely generated and changed at regular intervals to prevent password guessing and brute force attacks.
- Encrypt communication channels to secure authentication tokens when possible.
- If your corporate account has become compromised or if a device that has cached credentials is lost or stolen, suspend MFA for remembered devices and browsers.
- Set up Azure Conditional Access for SaaS applications, which allows the configuration of per-application multi-factor authentication access rules.
- Ensure the need for app passwords for non-browser clients.

2. Use appropriate access controls

Access control is a mechanism for providing a user who has a valid identity, and who has authorized rights and/or privileges, to access and perform functions using information systems, applications, programs, or files. Comprehensive access control strategies need to be in place, especially when considering the fact that corporate employees expect to work from any location, on devices of their choice, and to seamlessly connect and access business applications.

Microsoft Azure Active Directory Access Control (ACS) is a cloud-based service that provides a way to authenticate and authorize users to gain access to web applications and services, while allowing authentication and authorization to be factored out of code. Instead of implementing an authentication system with user accounts that are specific to an application, it’s possible to let ACS orchestrate the authentication and much of the authorization of users.

Common ACS functionalities include:

- Federation
- Authentication
- Authorization
- Single Sign Out
- Security Token Flow and Transformation
- Trust Management
- Administration
- Automation

Role-based access control (RBAC) features can be used to restrict access and permissions for specific cloud resources. To help detect suspicious access, Azure Active Directory offers reports that provide alerts about anomalous activity, such as a user logging in from an unknown device. In addition, operational logging and alerting capabilities can notify customers if someone stops a website, or if a virtual machine is deleted.

Recommendations:

- Secure inbound Internet communications to services using SSL.
- Register corporate devices with Azure AD.
- Set up Azure Conditional Access for SaaS applications, which allows the configuration of per-application multi-factor authentication access rules.
- Improve the quality of implementation from a security perspective by adhering to the ACS Security Guidelines. Also consider implementing retry logic when token requests to endpoints fail. Become familiar with ACS best practices for secure operations and development.
- Communication between on-premises hosts and cloud services should be authenticated, authorized, and encrypted using virtual Site-to-Site or Point-to-Site VPNs.

3. Use industry-recommended, enterprise-wide antimalware solution

Malware, also known as malicious code and malicious software, refers to programs that are inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system to annoy or disrupt the victim. Malware such as viruses, trojans, and worms are usually designed to perform nefarious functions in such a way that users are unaware of them, at least initially.

Microsoft Antimalware for Azure is a security extension that extends antimalware protection to virtual machines and to cloud services. The antimalware software used by Microsoft cloud services supports a fully centrally managed solution that includes real-time scanning of files that come in to the systems, automatic checks for updated signature files and software updates, and alerts to the Microsoft Operations Center (MOC) of detected malicious code.

Microsoft also employs intrusion detection, distributed denial-of-service (DDoS) attack prevention, regular penetration testing, data analytics, and machine learning tools to help mitigate threats to the Azure platform. Azure offers three options for antivirus/antimalware solutions on Azure virtual machines:

- Symantec Endpoint protection
- Trend Micro Deep Security as a Service
- Deploying antimalware

Recommendations:

- Deploy antimalware solutions on Azure VMs.
- Use the Antimalware solution in Microsoft Azure Operational Insights to report on the status of antimalware protection in organizational infrastructure.
- Establish and maintain general malware awareness programs for all users, as well as specific awareness training for the IT staff directly involved in activities that relate to malware prevention.

4. Effective certificate acquisition and management

A certificate is a form of identification for websites and web applications that is used to verify authenticity. Websites rely on TLS and Secure Socket Layer (SSL) to encrypt data communications. To securely configure TLS or SSL for an application requires a TLS or SSL certificate. Self-signed certificates can be acceptable in some restricted use cases (dev and test). However, a signed and authorized certificate that is issued by a certification authority (CA) or a trusted third-party who issues certificates for this purpose is recommended. Certificates can be obtained from a company that provides TLS and SSL certificates.

Azure uses certificates in several ways. For example:

- Management certificates. Stored at the subscription level, these certificates are used to enable the use of the SDK tools, the Windows Azure Tools for Microsoft Visual Studio, or the Service Management REST API Reference. These certificates are independent of any cloud service or deployment.
- Service certificates. Stored at the cloud service level, these certificates are used by deployed services.
- Secure Shell (SSH) Keys. Stored on the Linux virtual machine, SSH keys are used to authenticate remote connections to the virtual machine.
- Point-to-site and site-to-site VPNs into Azure resources require certificates for authentication and encryption.
- RDP connections to Windows-based virtual machines.

Recommendations:

- Certificates used in production systems should only be acquired from one of the reputable certification authorities (CAs).
- Certificates need to be configured with traceable information, including designated contacts, from a limited set of authorized users.
- Self-signed certificates as well general certificates should not be shared with or reused on systems that have a different application context.
- It is essential that certificates are treated as highly valued assets.
- Track expiration dates of certificates and keys. Because certificates and keys expire by design, it is important to track the expiration dates and take appropriate action prior to expiration so that applications that use ACS continue to function properly without interruption.
- Avoid embedding the IDs and secrets into applications. Consider applying the guidance provided as best practices for deploying passwords and other sensitive data in applications
- Secure keys by protecting them in a Key Vault, which encrypts keys and small secrets like passwords with keys stored in hardware security modules (HSMs).

5. Encrypt all customer data

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information is encrypted using an encryption algorithm, which generates cipher text that can only be read if decrypted. An encryption scheme usually uses an encryption key generated by an algorithm. BitLocker encryption can be used to protect data at rest, and Transport Layer Security (TLS) can be used to protect data in transit.

Azure offers rich security functionality, including deep support for standardized encryption protocols. Developers can use the cryptographic service providers (CSPs) built into the Microsoft .NET Framework to access Advanced Encryption Standard (AES) algorithms, along with Secure Hash Algorithm (SHA-2) functionality to handle such tasks as validating digital signatures. Moreover, the Azure platform builds on the straightforward key management methods incorporated into the .NET security model, so developers can retain custom encryption keys within the Azure storage services.

Azure allows customers to encrypt data and manage keys, and safeguards customer data for applications, platforms, systems, and storage.

- Protecting data at rest. Azure offers a wide range of encryption capabilities that provide customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps streamline key management and maintain control of keys used by cloud applications and services to encrypt data.
- Protecting data in transit. For data in transit, customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit, such as between two virtual networks. Azure strives to use industry accepted standard transport protocols such as TLS between devices and Microsoft datacenters, and within datacenters themselves when possible.

Recommendations:

- Encrypt data in storage and in transit to align with best practices for protecting confidentiality and data integrity.
- Ensure all devices, including BYOD devices, use protected transmission and storage capabilities.
- Encrypt traffic between web client and server by implementing TLS on IIS.
- Choose HTTPS for REST API (recommended) for storage.
- Use well-known encryption algorithms as provided in the .NET CSPs. These are proven and tested for security.
- Authentication tokens are often the target of eavesdropping, theft, or replay-type attacks. To reduce the success of these attacks, encrypt the communication channels.
- When designing web applications, use the secure design guidelines.
- Use Azure Key Vault to store secrets such as passwords with keys stored in hardware security modules (HSMs).

6. Penetration testing

Designers need to think like attackers when planning and designing an organization's network and services. Penetration testing is not about verifying functionality, but about verifying the absence of insecure functionality. Effective penetration testing is about finding properties in software and its environment that can be varied, varying them, and seeing how the software responds. The goal is to ensure that software performs reliably and securely under reasonable and even unreasonable production scenarios.

Recommendations:

- Work with a reputable penetration solution vendor.
- Perform tests on endpoints to uncover OWASP top 10 web vulnerabilities.
- When using Azure services, request for permission to execute penetration tests.
- Review methods in penetration testing also called red teaming.

- Help Azure become resilient to attacks by reporting potential security flaws related to Microsoft services.

7. Threat modeling services and applications

Organizations need to properly define threats and classify information assets with a threat-modeling process. The Microsoft Security Development Lifecycle (SDL) provides an effective threat-modeling process that is used to identify threats and vulnerabilities in software and services. Threat modeling is usually done during the project design phase but can be done anytime to bring exposure to possible threats.

Threat modeling is a team exercise, encompassing the operations manager, program/project managers, developers, and testers, and represents a key security analysis task performed for solution design.

Threat modeling activities include:

- Completing threat models for all functionality using the SDL Threat Modeling Tool, which can be used to identify high-risk issues.
    - Modeling the service design and enumerating STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) threats across all trust boundaries has proven an effective way to catch design errors early on.
- Threat modeling all services and projects. All code exposed on the attack surface and all code written by or licensed from a third party should be included in a threat model.
- Ensuring that threats can be mitigated and reviewed by the team.
- Reviewing a threat model when software is updated. New features or functionality can change the solutions threat profile.
- Endeavoring to build secure solutions with the mindset that they are trying to protect their customer's assets.

Recommendations:

- Use approved tools, software, and services. Ensure that only verified tools are used in solutions.
- Remove and deprecate unsafe functions, processes, and designs.
- Perform fuzz testing, static, and dynamic analysis of services and software solutions.
- Conduct attack surface analysis and reviews.
- Learn and understand how exploits and vulnerabilities might affect an organization by reviewing security threat intelligence.
- Apply threat modeling best practices as appropriate to current, new, and third-party services and applications.

8. Log security events, implement monitoring and visualization capabilities

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries. Each entry contains information related to a specific event that has occurred within a system or network. A forensic analysis uses a security and audit solution seek out evidence that potentially malicious users leave behind. Regardless of what users do in their IT environment, many of the activities they participate in generate security artifacts. Evidence about their use is stored in event logs.

Azure Operational Insights collects these artifacts *as soon as they occur*, before anyone can tamper with them, and allows different types of analysis by correlating data across multiple computers. Azure enables customers to perform security event generation and collection from Azure IaaS and PaaS roles to central storage in their subscriptions. These collected events can be exported to on-premises security information and event management (SIEM) systems for ongoing monitoring. After the data is transferred to storage, there are many options to view the diagnostic data.

Azure built-in diagnostics can help assist with debugging, and Azure security and audit log management refers to how you can set up logging effectively to monitor your Azure subscription. For applications that are deployed in Azure, a set of operating system security events are enabled by default. Customers can add, remove, or modify events to be audited by customizing the operating system audit policy.

Recommendations:

- Refer to the Security Policy Settings guidelines to implement and manage security policies for Windows-based virtual machines running in Azure IaaS.
- Enforce the right settings to ensure that Azure instances are collecting the correct security and audit logs.
- Monitor the Overall Health of an Azure instance through *Azure Status*.
- Monitor Media Services through the *Azure Media Services Dashboard*.
- Monitor Cloud Services and Storage Account through the *Azure Management Portal*.
- Monitor Web Apps in *Azure App Service*.
- Monitor Hadoop Clusters in HDInsight using the *Ambari API*.
- Store service data and security log data in separate storage accounts. This isolation ensures that saving security log data does not affect the storage performance for production service data.
- Monitor Azure Data Factories using *Data Factory .NET SDK*.
- Protect and audit log files in virtual machines running in Azure IaaS using Windows access control lists (ACLs).

9. Determine the root cause of incidents

Root cause analysis (RCA) is a structured and facilitated team process used to identify root causes of an event that resulted in an undesired outcome. The end result of this exercise is to develop corrective actions that can be driven back into policy. The RCA process provides a way to identify breakdowns in processes and systems that contributed to the event and how to prevent future events. The purpose of an RCA is to find out what happened, why it happened, and determine what changes need to be made. Organizations need to be prepared to investigate a breach and provide a root cause analysis of the breach – that is, thoroughly documenting the breach, how it happened, and specifically what has been done to address the security issue so that a breach doesn't happen again.

Operational Insights, as part of the Microsoft Operations Management Suite, is a software as a service (SaaS) solution tailored for IT operations teams. This service leverages the power of Azure HDInsight to collect, store, and analyze log data from virtually any Windows Server and Linux source, from any datacenter or cloud, and turn it into real-time operational intelligence to enable better-informed decisions.

Recommendations:

- Monitor high risk Windows events within virtual machines running in Azure IaaS for better root cause analysis.
- Establish aggressive audit policies within virtual machines running in Azure IaaS.
- Adhere to and understand best practices for forensic analysis, security breach pattern investigations, and audit scenarios.
- Use the Security and Audit solution in Microsoft Azure Operational Insights to conduct a simple investigation for a suspicious executable.

10. Train all staff in cyber security

If a development team does not understand the basics of secure design and development or the risks of running web-based solutions and services, security training is imperative and should be completed before any Azure-based application is designed, built, tested, or deployed. All members of the operations and development teams should be informed about security basics and recent trends in security and privacy, and they should attend at least one relevant security training class every year at a minimum.

Staff and vendors should be encouraged to seek opportunities for additional security and privacy education when possible. Employees that are well-versed and up-to-date on security issues are better able to design, develop, and operate software with security in mind first.

Organizations must ensure that the software they create or acquire includes the security properties that are required to meet their current and evolving business and compliance needs. Accomplishing this goal requires that skilled individuals have a clear understanding of software security with respect to applicable business objectives and technologies in use, along with the skills required to specify, develop, test, and field the software appropriately.

A commitment to understanding security basics and the latest developments in security and privacy can greatly help organizations reduce the number and severity of exploitable software vulnerabilities, as well as to react appropriately to ever-changing threat landscapes.

Recommendations:

- Create an internal security awareness website to provide resources to communicate policy best practices and safety tips throughout the organization. Brief email bulletins can help reinforce and promote key security concepts, including step-by-step guidelines.
- Remember to keep it simple, and recognize that most employees are hired to support the business and not for their IT expertise. The key concepts of security, privacy, and information protection must be taught.
- Executive-backed security policies that all employees must comply with will help protect customer and company data.
- Make security interesting. Intranet webpages can teach users home safety in avoiding scams, malware attacks, and information disclosure. Help users take their security training home. Teach users to keep their home systems up-to-date and secure, which will help improve the organization's overall security posture.
- Provide brief, highly focused training sessions that are based on real events. Sharing key learnings can help users understand the risks.

11. Patch all systems and ensure security updates are deployed

Software systems need to be updated with necessary security updates regularly. Organizations need to watch out for security threats and maintain stability of software environments. Minimizing security threats requires properly configured systems that use the latest software and have the recommended software updates/patches installed.

Microsoft has developed various solutions to help organizations that have varying needs to stay as up-to-date as possible within their own specific environments. Through the Automatic Updates feature, and when customers opt in through Microsoft Update, Windows can automatically keep computers up-to-date with the latest security updates for all Microsoft products. Users do not have to search for updates and information.

Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software.

Recommendations:

- Enable Windows Update or use Windows Server Update Services, which provide recommendations to upgrading systems and to ensure they are up-to-date.
- Update all third-party applications, and use their patching capabilities when possible.
- Get security updates from the Microsoft Download Center.
- Review the best practices for applying service packs, hotfixes and security patches.
- Get updates for consumer platforms, such as Microsoft Update designed to update Microsoft products.
- Get the latest information on security-related patches.
- Follow the Security Development Lifecycle (SDL) recommendations to build more secure software and address security compliance requirements while reducing development cost.
- Enable notifications for new updates and reporting functionality based on update status, computer status, computer compliance status, and update compliance status.
- Review the Microsoft Security Update Guide to learn more about Microsoft Updates and Windows Server Update Services.
- Follow the Software Updates Security Best Practices.
- Use the System Update Assessment solution in Microsoft Azure Operational Insights to report on the status of updates applied to infrastructure.

12. Keep service and server inventory current and up-to-date

Service and server inventory is about knowing what subscriptions, domains, services, networks, and hosts are owned and managed. Keeping track of the services and mitigating the risks that come with those services is key for secure operations. In addition, have an understanding and priority of the data that is being protected by implementing a data classification effort, as described in the Data classification for cloud readiness white paper.

Recommendations:

- Establish information classification.
- Identify data flows between integrated systems.
- Maintain documentation to reflect changes in inventory.
- Run network discovery to help identify hosts and networks in the organization’s IP range.

13. Maintain clear server configuration with security in mind

Server misconfiguration is one of the most common causes for unauthorized users accessing and compromising the host. Because of the potentially complex security configuration requirements, it’s essential to use a master server image that has security measures in place. Azure provides customers a marketplace with a gallery of servers that have been configured with security in mind. However, the use of the servers in the marketplace requires attention when organizations require custom security modifications and to prevent security configuration drift.

If a custom VM image is created, it’s essential that the virtual machines have a standard set of baselines applied to them. The Microsoft Security Compliance Manager provides a means to create a standard baseline and deploy *the baseline to existing servers, as well as create a master, or gold, image enabling security capabilities.*

Microsoft Baseline Configuration Analyzer *(MBCA) can help identify and maintain optimal system configuration by analyzing configurations of computers against a predefined set of baselines designed by the security configuration manager, reporting results of the analyses. Best practices are packaged in the form of a best practice model kits. The kits are set of best practice configurations recommended for customers to use. Models are available as separately downloadable packages that can be run and analyzed by MBCA.*

It's possible to test deployments using the Azure Best Practices Analyzer (BPA) for Azure Pack*. BPA is a tool that analyzes the components of Azure Pack. It helps immediately identify many configuration, security, and performance issues, and it recommends best practices to resolve them. BPA for Azure Pack works within Microsoft Baseline Configuration Analyzer (MBCA) to* scan the software configurations *of the computer on which it is installed. It automatically detects all components that are installed in Azure Pack and compares their configurations against a set of rules. MBCA then lists all noncompliant issues.*

Recommendations:

- Protect domain and local administrative accounts with strong passwords and MFA.
- Use the Secure Administrative Hosts feature to administer servers.
- Allow RDP connections only from specific IPs by enabling Azure MFA white listing of administrative computers.
- Configure auditing events, monitor the failed logon attempts, and block the IPs.
- Configure auditing for failed logon events such as 4625 and 4648 and configure alerts or schedule tasks to run a batch file to extract the IP from the event log entry and block it by adding a firewall rule.
- Don't use the same password for all virtual machines. Change the passwords frequently.
- Run best practices analyzer and take appropriate action to fix security issues reported by the tool.

Applying key principles a Lift and Shift use case

Use cases are presented to help illustrate how to incorporate the thirteen key principles and recommendations for secure development and operations into a solution design with compliance considerations. Each consideration will present a description, requirements for the solution, and how the key principles align to solution requirements.

The requirements focus will be on considerations for handling PII and/or PHI data. The use case will NOT have the depth that is found in all-up architecture design patterns for availability, scalability, and disaster recovery requirements as are available here, as an example. This is a complementary resource with considerations around security and compliance. The focus is to apply the concepts presented in this paper to a use case.

Keep in mind that there are many ways to solve a particular use case. You should carefully consider all the requirements of the application and all relevant aspects for meeting your own compliance obligations.

As a user of Azure, you should independently verify with your own legal counsel that your implementation meets all local compliance regulatory requirements.

Implementation of a healthcare application

The idea of the 'lift and shift' implementation is based on the principle of moving an application's services and data from on-premises to a cloud-enabled model with few if any changes to any applications.

This example migrates an electronic medical records (EMR) system built in C# running on a Windows 2012 R2 server virtual machine. The migration will require moving the application to an Azure IaaS environment. Because the code base is available, a choice was made to create the IaaS environment new and not migrate the virtual hard drive (VHD) itself. A benefit of this approach is upgrading to the latest version of the operating system, because there are no direct dependencies. The plan is to take advantage of the SQL PaaS offering in Azure and migrate the data from the on-premises SQL 2012 R2 server.

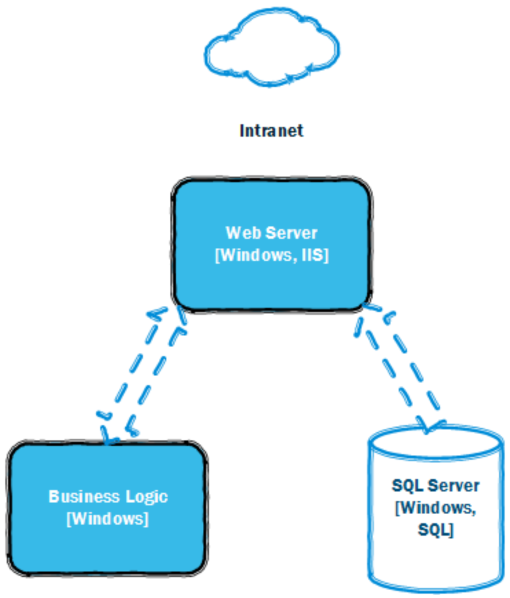
Because a lift and shift implementation tries not to change the system, it is not unexpected that security-related issues, whether known or not, will come along from on-premises to the cloud. However, because the cloud is visible, it is perceived as having a much larger attack surface than an on-premises environment. Understanding and deliberately applying sound security practices when adopting the cloud should be part of the early design.

The example addresses a fictitious company called Contoso that has provided EMR solutions to small physician offices and medical clinics for about five years. Their product has been well-received and the company has done well. As Contoso's business grew, they had to keep expanding their operations team to meet the demands of their new customers. It soon became evident that having an on-premises solution required putting staff on site to install the system and then spending several weeks configuring the application to match the customer's business practices. It was also noted that new releases were putting a heavy burden on the operations staff.

The Contoso leadership team determined that changes were required so they could reduce operational overhead and at the same time increase profits. Having heard about the cloud, they decided to reach out to Microsoft and discuss potential solutions to meet their goals while ensuring that the handling of their customers' personally identifiable information (PII) and personal health information (PHI) data was handled properly.

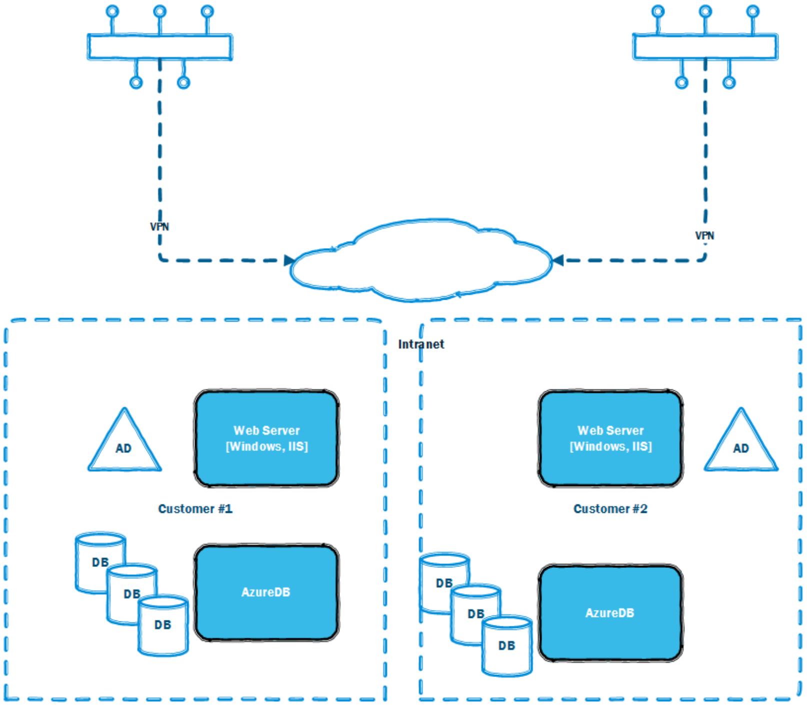
After a number of architectural and technical discussions, the decision was made to have two (2) work streams; the first was a lift and shift of the existing application to Azure, and the second was to begin work on a new multi-tenant built-for-the-cloud application. This discussion will therefore focus on the lift and shift effort.

The following illustration represents the architecture of the EMR solution as deployed at each customer's site. It is a very simple deployment; the application is a web-based experience and the business logic is part of the web application.



As discussed below, there are a few changes taking place as part of the move to Azure. These changes are being done to help enhance security and access controls, as well as to take advantage of the data replication capabilities of Azure.

The Azure deployment architecture is illustrated in the following figure.



The move to Azure still has each Contoso customer having their own set of servers and databases. However, because they are all collocated in the Azure data centers, it is possible to monitor these servers together and to address updates and installations thru automated mechanisms, such as through Azure automation and scripts, without having to visit the customer's site

The use case presents many requirements for the solution to consider. The following table lists 22 requirements identified by Contoso as important for successful migration:

1. User authentication	7. Protect access from external systems	13. Protect against malware	19. Training
2. Protect data in-transit	8. Protect secrets	14. Identity management	20. Patching
3. API protected by credentials	9. DR plan	15. Threat modeling	21. Inventory
4. Audit CRUD operations	10. No activity handling	16. PEN testing	22. Server configuration
5. Protect data at rest	11. Protect data from external systems	17. Log security events	
6. Protect access to data	12. Monitor network traffic	18. Incident root cause	

Solutions requirements

Azure IaaS

Azure Virtual Machines allow the deployment of a wide range of computing solutions in an agile way. With Azure Virtual Machines, it's possible to deploy nearly instantaneously and pay only by the minute. With Windows, Linux, SQL Server, Oracle, IBM, SAP, and BizTalk, it's possible to deploy any workload, in any language, on nearly any operating system.

More information on virtual machines can be found here.

Azure SQL Database

Developers who build software as a service (SaaS) applications can leverage SQL Database to provide flexibility and to support both explosive growth and profitable business models. For workloads with unpredictable database resource consumption, the elastic database model provides the ability to pool resources to be leveraged among a group of databases. Instead of overprovisioning to meet peak demand, an elastic database pool can let hundreds or thousands of databases leverage resources within a controlled budget. It's possible to drive cost efficiencies with a purchase model that provides control over price and performance across a group of databases.

More information on SQL Database can be found here.

Azure Active Directory

Azure Active Directory (Azure AD) is a multi-tenant cloud-based directory and identity management service from Microsoft.

For IT Admins, Azure AD provides an affordable, easy-to-use solution to provide employees and business partners with single sign-on (SSO) access to thousands of cloud SaaS applications such as Office365™, Salesforce.com, DropBox, and Concur.

Azure AD lets application developers focus on building applications by making it fast and simple to integrate with a world-class identity management solution used by millions of organizations around the world.

Azure AD also includes a full suite of identity management capabilities, including multi-factor authentication, device registration, self-service password management, self-service group management, privileged account management, role-based access control, application usage monitoring, rich auditing, and security monitoring and alerting. These capabilities can help secure cloud-based applications, streamline IT processes, cut costs, and help ensure corporate compliance goals are met.

More information on Azure AD can be found here.

Key principles applied to solution requirements

In the following subsections, each key security principle section considers the application requirements, which may handle PII, PHI, or general security and presents decisions and considerations for the use case application. Keep in mind that the Key Principles section offers recommendations that can be further incorporated to harden the requirement.

A snapshot of how the thirteen key principles aligned to this use case's 23 design requirements help to align how a solution architect and a compliance officer may consider the security controls applied in the design:

Key Secuirty Principles Use Case Solution Requirements	Identity & Authentication	Access Control	Anti-Malware	Certificate Acquisition & Management	Data Encryption	Penetration Testing	Threat Modeling	Logging	Root Cause	Train staff in cyber security	Patch System	Service/Server Inventory	Secure Server Configuration
1 -User Authentication	x												
2 - Protect data in-transit					x								
3 - API protected by credentials	x			x									
4 - Audit CRUD operations								x					
5 - Protect data at rest					x								
6 - Protect access to data		x											
7 - Protect access from external Systems		x											
8 - Protect secrets	x			x									
9 - DR plan	x			x	x								
10 - No activity handling		x											
11 - Protect data from external systems		x			x								
12 - Monitor network traffic								x					
13 - Protect against malware			x							x			
14 - Identity Management	x												
15 - Threat Modeling							x						
16 - PEN testing						x							
17 - Log security events								x					
18 - Incident root cause									x				
19- Training										x			
20 - Patching											x		
21 - Inventory												x	
22 - Server configuration													x

Identity and authentication

Healthcare solution design implications: Identity and authentication play a critical role in the healthcare space. Specifically, regulations and privacy concerns point toward having clear and verified knowledge of who is accessing health information. This identity has a significant role in auditing actions/work done on a patient's records as well as being key in determining access rights to patient data.

Doctors, medical assistants, nurses, and office staff must be able to authenticate (log in) in a secure way

With increasing regulatory pressure, every healthcare organization will need to enhance their security access to their critical systems and sensitive health care information. Healthcare organizations need to implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. They also must determine threats and vulnerabilities to authentication of persons or entities that seek access to its electronic protected health information, and mitigate risks by establishing verification techniques to ensure that the person or entity seeking access to such information is the person or entity claimed.

Although the application that ran on-premises used a custom, homegrown authentication method, the decision was made that this approach was not as secure as what the ISV's customers would want of an application that runs in the cloud. Therefore, it needed to be modified. NOTE: Occasionally in a lift and shift scenario, targeted pieces of an application may be updated to address operations, performance, or in this case, security needs.

Recognizing that there are several identity and authentication standards today that are accepted as secure, the decision was made to use Azure Active Directory (AAD), a standard service offered in Azure, which takes advantage of these well-understood standards. Specifically, the choice was made to use OpenID as the protocol for authenticating users.

Because the original application was written several years ago and because detailed threat modeling wasn't really ever done, the decision was also made to require multi-factor authentication as a safeguard to reduce the likelihood of a hacker gaining access to the application. Although MFA allows for trusting a device after it is registered, the team made the decision to require MFA whenever a user signs in.

As a lift and shift single-tenant application, each customer will have separate server instances allocated specifically to them. Azure Active Directory will be configured as single-tenant, which keeps the application registry and users defined in the same directory store. As a result, no specific consent process will need to be performed.

Role-based access controls (RBAC) within Azure Active Directory will not be used for this application because authorization management already exists in the application via a custom service and data store.

Because all authentication requests, both success and fail, are logged/audited, it will be possible for the security team to analyze the logs and look for possible instances of intrusion detection.

Strong password policies help make the application more resilient to brute force attacks, and enabling multi-factor authentication functionality helps protect against attacks that take advantage of password guessing.

No part of the system should be callable (for example, mobile devices retrieving data) without secure credentials

To deploy this application as quickly as possible to Azure, the decision was made that any access to the application must come in over the VPN. This approach means that the customer has taken responsibility to address how its users can use devices to access their internal network and then connect over VPN to the EMR application.

In addition, whether mobile or not, all users will authenticate via Azure Active Directory and will be subject to the rule established for multi-factor authentication.

All storage keys must be protected so that they can't be accidentally disclosed

Many data services in Azure use an identifier and secret to access storage. There are tokens that can be used as well for some services that have time to live (TTL) with access rights encoded into them. A common mistake is embedding the IDs and secrets into the application because it can lead to disclosure of the keys and ultimately the data; also, managing the storage keys is complicated because they are distributed in many places.

To protect the keys needed to read the data, the decision was made to take advantage of Azure Key Vault, an HSM-backed service that encrypts and protects secrets. With positive authentication required to get access to the key vault, the application's secrets can remain secret.

System must have a disaster recovery plan that guarantees that the data/information is protected

Power outages and loss of Internet connectivity can prevent clinicians from accessing patients' records, and it can be very difficult to treat patients without appropriate data. Disaster recovery in healthcare is a fine art of balancing cost and uptime. Unfortunately, healthcare organizations face significant costs to upgrade their technical infrastructure and most of them end up not implementing it, which can lead to significant issues and failures.

One of the benefits of using Azure is that storage is copied three times in the datacenter where the storage account is defined. Also, by using Azure SQL PaaS, the application benefits as SQL PaaS has built-in high-availability. In addition, Azure offers a standard disaster recovery plan in case of a datacenter loss.

Customers need a secure way of managing access identities and roles

Azure Active Directory can be managed through the Azure portal, which requires authentication and permissions. In addition, there are add-on tools for managing identities.

Access control

Healthcare solution design implications: Access control is essential to provide for the confidentiality of the EMR because it is part of the authorization process where the system checks if the user can access the requested resources. Access control is an important aspect of information security that is linked to the main information security characteristics such as confidentiality, integrity, and availability.

When the system has positively identified who is connecting to the system, it is critical to ensure that any authorized requests are allowed. Verifying that a person can perform some operation against some piece of data is essential to protect privacy and to ensure that only the appropriate people can access specific data, such as one of the doctor's patients. Consider also that adding some data to a patient record can result in mistreatment and/or death. In this case, it is critical that only the appropriate authorized people have access to modify the patient record.

All information transmitted over a public network (Internet, office network, cell) must be protected to avoid accidental disclosure

In the lift and shift example, the implementation of access control mechanisms starts with the implementation using secure inbound Internet communications to virtual machines. The current on-premises solution made use of SSL, which is considered secure, but the decision was made that communications between on-premises and cloud services should be encrypted using site-to-site, or point-to-site VPN encryption when transmitting PII or PHI data. NOTE: A VPN isn't necessarily required, but the feeling was that having one in place would reduce risk of inadvertently opening a security hole in the customer's network.

All devices that will be on the network need to be registered on the corporate network with Azure AD. In addition, Conditional Access for SaaS applications, which allows the configuration of a per-application multi-factor authentication access rule, will be enabled.

All access to data, whether read or write, must be verified to ensure that the user has the authorization to access the data

Patient data is sensitive and should only be accessed by authorized clinicians or administrators with appropriate rights. For example, for verification of claims, administrators need only READ access while physicians might need WRITE access to update and maintain the patient records.

The application has an existing authorization system that manages users' permissions to access data, and tracks access rights to patient data. The one piece that probably will need to be updated is the migration of the users' unique identities, which would then connect the immutable identity id, which is defined in Azure Active Directory, to the authorization table.

All access to the system from external systems must be authorized

There are several ways to solve this scenario, depending on how many external systems are allowed and what they are doing. The ISV who wrote this application has decided that because the current external users are coming through to REST services, they will require that the external system authenticate via Azure Active Directory using a X.509 certificates.

When no activity is detected for >2 minutes from a device, the user is logged off

Most clinicians log out of the system when they leave the room after the consultation; this is standard practice that has been adopted in the industry. To safeguard against clinicians not logging out, timed logout is enabled in applications which automatically logs out after specific time of no activity.
Taking advantage of the authentication token and associated cookie, the application can set a TTL such that no activity will cause the token to be invalidated and require the user to have to re-authenticate.

Data storage must not be accessible directly from external users

Taking advantage of a capability in Azure SQL PaaS, an access control list (ACL) can be defined that only allows for specific IP ranges to have access to SQL. This approach ensures that only the application servers running inside of Azure can have access.

Antimalware

Healthcare solution design implications: Malware is an everyday occurrence, but for busy healthcare providers the additional overhead of ensuring that their antimalware is up-to-date can easily become forgotten. There are so many other aspects to protecting patient records that need to be addressed, but malware protection is fundamental and needs to become a priority. Malware is not only a security issue in general, but when a system incurs a long window of time between updates, it will also introduce unnecessary risk. In many cases, healthcare providers do not have the bandwidth to address it. The result is that many systems in healthcare are still highly susceptible to common and preventable malware attacks, which can result in systems not performing to their best ability. Such a condition could compromise patient care if a system is infected, in addition to compromising patient and medical records.

System should guard against malware

Azure offers an antimalware solution that can be added to an IaaS VM, which makes it a great fit for this application.

Certificate acquisition and management

Healthcare solution design implications: In addition to having positive identification for users, it is also important for services and servers in the system to positively identify themselves before calling other services. This precaution minimizes DDOS and intrusions that could compromise data, cause the accidental disclosure of data, or worse. Certificates are a best practice for identifying services, and provide a means to prevent compromise.

Data encryption

Healthcare solution design implications: Healthcare and the associated compliance requirements call for the protection of data in transit and at rest. Using SSL or TLS will provide data protection in transit. Data at rest should be encrypted with AES-256 or better to achieve the best levels of protection. The underlying reason for protecting healthcare records is to ensure the continued privacy of patient data. By using rotating keys and different keys for each tenant, it is possible to further ensure that a loss of one piece of data doesn't expose other data.

All data at rest containing patient data, PII, or PHI must be protected so that hacking, loss of media, and similar events do not disclose information

It is important to remember that protecting data at rest with encryption does not stop hackers or someone trying to gaining access to data with malicious intent. What encryption does is stop or at least reduce the chances of data disclosure. HIPAA recommends the use of the AES-256 encryption algorithm, which provides for a level of data encryption that should be good for 10 years. It is strongly recommended that each instance of the EMR use a different encryption key to protect each customer's data separately. In this way, a compromise of data doesn't affect other customer's data.

Both SQL in IaaS and AzureDB (SQL PaaS) offer Transparent Data Encryption (TDE), which encrypts the data at rest for SQL-based data stores. This capability is enabled to protect the data from outside access.

If the example application was performing encryption, additional controls would need to be put into place to keep the keys locked in a vault, such as Azure Key Vault, where the keys themselves are locked and protected through the use of PKI (or asymmetric keys) and hardware security modules (HSMs). In addition, Azure provides HSMs that can be used with the Azure Key Vault service. It's important to also consider rotating encryption keys regularly.

System must have a disaster recovery plan that guarantees that the data/information is protected

Hurricane Katrina was a clear example of a natural disaster during which recovery of data would have helped immensely for better patient care. All healthcare organizations need to have a proper disaster recovery plan and be prepared to deal with such disasters. Treating patients with wrong data or no data could have dire consequences.

Data storage must not be accessible directly from external users

Taking advantage of a capability in Azure SQL PaaS, an access control list (ACL) can be defined that allows for specific IP ranges to have access to SQL. Only the application servers running inside of Azure can have access.

Penetration testing

Penetration testing can be used to validate and verify potential weakness in infrastructure and software solutions. Identifying a reputable penetration solution vendor is essential, as is validating that endpoints are tested to uncover OWASP top 10 web vulnerabilities.

NOTE: When using Azure services, customers can requests for permission to execute penetration tests and reviewing the penetration testing methodology used by Azure need to be considered. If a potential security flaw related to Microsoft services is discovered, report it to the Azure response team.

Threat modeling

Healthcare solution design implications: It's essential that healthcare solutions be implemented using licensed and approved tools, software, and services. Licensed solutions tend to reduce the risk of being infected with malware; also, vendors will tend to patch current software against vulnerabilities. Using an unauthorized or unsafe solution may increase risk and exposure to malware. Also it's essential to deprecate unsafe functions, processes, and designs.

When getting ready to design a solution it's beneficial to understand the threat landscape, which can be done by reviewing security threat intelligence.

Also, new applications should be designed by applying threat modeling best practices, conducting attack surface reviews, and running fuzz testing, static, and dynamic analyses of services and software solutions prior to deployment into production.

Logging

Healthcare solution design implications: There are healthcare compliance requirements that stipulate that all changes to patient records be logged/audited to track what data has been added or changed, who did it, and when that change occurred

All updates to the system will be audited with date/time, user who modified the data, what was done

The on-premises solution used Microsoft SQL Server for managing all data used in this application. As part of the migration to Azure, the team was able to take advantage of the Azure SQL PaaS offering for logging.

Root cause

Healthcare solution design implications: Root Cause Analysis (RCA) has been applied to the healthcare industry and has been found to be a highly effective tool to improve patient care and reduce healthcare costs from adverse events. RCA is a systematic and comprehensive methodology to identify the gaps in a hospital's systems and processes of care that may not be immediately apparent and that may have contributed to the occurrence of an incident.

Determine the root cause of incidents

As described in the Incident Response section, an incident response plan needs to be in place for all solutions and applications. As best practices, consider forensic analysis, security breach pattern investigations, and audit scenarios.

Train staff in cybersecurity

Training requires a multi-faceted approach. However, the key elements to consider are:

- Create a security intranet website.
- Keep the communications simple and effective.
- Make people accountable for maintaining a level of security awareness.
- Ensure that your executives are on board, and provide support to a security champion.
- Inform your operations and development team with formal training such as the SDL training.

Patch systems

The example ensures that Windows Update is enabled, which will ensure that a system that uses ActiveX technology to scan the PC will determine what has been installed and present a list of suggested components that need upgrading based on the most up-to-date and accurate versions. Software systems need to be updated with necessary security updates regularly. Organizations need to watch out for security threats and maintain stability of software environments. Minimizing security threats requires organizations to have properly configured systems, to use the latest software, and to install the recommended software updates/patches.

Service/server inventory

Keep your service and server inventory current and up-to-date

Having good insight into what needs to be protected is essential when moving an application to Azure. Before beginning the process, create a basic questionnaire to verify anything that will store, process, or communicate PII or PHI, such as financial, medical, or sensitive customer information. The Data classification for cloud readiness white paper provides simple guidance to classify data, including PII and PHI data, for management.

Secure server configuration

Maintain clear server configuration with security in mind

Server and cloud service management with well-defined configurations is essential to prevent unauthorized use of PII or PHI. Protecting administrative and local accounts with strong passwords and MFA needs to be implemented as outlined in the identity and access recommendations.

It's also strongly recommended that secure access workstations be provided to server administrators, which will make it more difficult to breach the cloud services. Administrators should also create unique passwords for virtual machines, and change the passwords frequently.

When enabling connections, it's recommended that RDP connections be enabled only from specific IPs by enabling Azure MFA white listing of administrative computers. Key audit items to consider include:

- Configure auditing events, monitor the failed logon attempts, and block the IPs.
- Configure auditing for failed logon events such as 4625 and 4648 and configure alerts or schedule tasks to run a batch file to extract the IP from an event log entry and block it by adding a firewall rule.
- Run best practices analyzer and take appropriate action to fix security issues reported by the tool.

Conclusion

Cloud computing offers tremendous opportunities in healthcare to enable increased quality and greater access at lower cost. When healthcare providers and ISVs consider moving a portion of their infrastructure to Microsoft Azure, they have to evaluate their overall privacy, security, and regulatory compliance posture. This guidance is provided as a way to approach that migration with the use of international standards, understanding of compliance requirements, the principle of shared responsibilities, and rationalized mapping to address necessary controls.

Taking these concepts and applying them to use cases further illustrates how to approach cloud adoption in regulated industries.