Microsoft

Embracing Cloud in Health: a European Risk Assessment Framework

A guide to privacy and security considerations for the adoption of cloud services in the health sector

This document is open to consultation

December 2014

Legal Disclaimer

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

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

Acknowledgements

Contributors and Reviewers
Leslie Sistla, Elena Bonfiglioli, Ray Pinto (LCA), Marie Charlotte Roques Bonnet (LCA), and Anand Gaddum (iLink).

Table of Contents

Executive Summary

New technologies are enabling patients, clinicians and employees to be connected as never before across organisations. As the use of cloud computing, mobile devices and social technologies becomes more commonplace, and new streams of big data flow into the enterprise, the need to effectively manage end-to-end security, privacy and adherence to regulatory compliance becomes even more critical.

While the adoption of cloud computing offers many benefits for organisations in the health sector, such as the opportunities to improve quality of care, access to care, increase services and to reduce costs, it must be balanced with a rationalised assessment of risk in protecting personal health information and data. Individual country's data protection and health information-specific laws and regulations define security and privacy requirements within an organisation to ensure protection of personally identifiable health data by limiting the use, disclosure of and access to sensitive health information. When Microsoft Cloud Services are adopted by an organisation, there is joint or shared responsibility in meeting these requirements. Microsoft takes this responsibility very seriously.

This framework is intended as a guide for Chief Security Officers (CSOs), Chief Risk Officers (CROs), Data Protection Officers (DPOs), Compliance Officers and IT executives who are charged with managing risk and meeting regulatory requirements. Understanding that ultimately the obligation of meeting regulatory compliance lies within the health organisation, this paper offers insight into how the Microsoft Information Security Management System (ISMS) and other Microsoft initiatives can assist those organisations as they move to the cloud. In addition to the third party audited industry certifications and attestations, understanding Microsoft's approach to privacy and security risk management more broadly can help organisations in the health sector to assess and manage their overall risk when using Microsoft Cloud Services.

Proactive Approach to Risk Management in European Health Sector

In today's rapidly evolving IT environment, information security and data protection is critical. There is a necessity to move from a reactive threat-based risk management to more proactive and efficient risk management in order to better protect against looming security incidents and attacks.

Enterprise risk management for health organisations spans both clinical and administrative activities. Information technology and its increased use in clinical settings (EMR, analytics, telemedicine) makes managing that sensitive data particularly important in risk management for the health sector.

Legislative Framework

Around the world, organisations operating in the health sector are mandated to follow local regulatory laws when handling personally identifiable data. Failure to follow these regulations can result in fines, reputational damage and possible imprisonment in some countries. In the EU, these regulations derive from the data protection framework, set out in the EU's Data Protection Directive 95/46/EC and national implementing legislation, and from local health information-specific rules and regulations. The legislative framework is supported by authoritative guidance provided by national data protection authorities (DPAs) and other regulatory bodies, such as the Article 29 Working Party, a group that brings together all 28 EU Member State DPAs.

Fundamental Principles of EU Data Protection Law

EU data protection law imposes different obligations on "controllers" and "processors".

Cloud customers that decide to move their data to the cloud remain "**controllers**" of the transferred data and have the ultimate responsibility for ensuring that personal data is processed in compliance with substantive requirements of the applicable data protection legislation. These requirements include, among other obligations:

- ensuring that personal data is only processed for **specified, explicit and legitimate purposes**,
- implementing appropriate **technical and organisational measures** to protect personal data, and
- complying with **cross-border transfer rules** where personal data is transferred outside the European Economic Area (EEA) **(**e.g., via the **European Commission's Model Clauses**).

Cloud service providers are considered "**processors**" that handle personal data on behalf of and pursuant to instructions from their cloud customers. While processors are not directly subject to the substantive requirements of the EU's data protection framework, they do have a duty to ensure **confidentiality of the data** in the cloud.

The Article 29 Working Party has made it clear that organisations must choose a cloud service provider that is able to assist them to comply with data protection legislation. The contractual framework between the cloud customer and cloud provider plays a particularly important role to that effect.

In addition to the general data protection laws that apply to all personal data, EU Member States also typically have local rules and regulations that apply to health information specifically. While such rules and regulations differ among countries, the common objective of such rules is to ensure the confidentiality and security of sensitive health information regardless of the medium and location in which the data is processed.

These national data protection and health information-specific laws and related regulatory guidance generally require or encourage organisations to establish a strategy for assessing risk and managing information security. As an example, the Article 29 Working Party's Cloud Opinion 05/2010 explicitly states that "a precondition for relying on cloud computing arrangements is for the controller to perform an adequate risk assessment exercise" and for cloud service providers to provide the cloud customer with all the information that is necessary for such an exercise. Similarly, in the UK, all public health organisations are required to carry out an information governance assessment of third party service providers and their services when such services involve the transfer, storage or other processing of personal data.

Information Classification

The first step in ensuring that an organisation's sensitive information is adequately protected is identifying the information involved. An understanding of the specific data in issue is key to determining how that data should be protected. Thus, an effective information classification and management process — which entails identification and classification of information assets against a defined taxonomy — forms an integral part of any data privacy and security risk assessment exercise. This process enables organisations to ensure that the correct level of control is applied to key or sensitive information. Organisations that fail to effectively identify and classify their information assets will typically treat all data sets the same regardless of their sensitivity and value, which often results in inaccurate and ineffective risk assessment and management strategies for the organisations' data. Significantly, the EU is working now on updates to its data protection laws. New rules may require all data controllers and data processors to maintain an inventory of the categories of personal data they process, making information classification even more important.

Data classification assists organisations in deciding what data can appropriately be stored and processed in different IT architectures, such as on premises versus in the cloud. For many organisations, "hybrid cloud deployment" will make sense; in this environment, some information and IT functionality will be stored and operated in public clouds and more sensitive information that cannot for compliance, privacy, business or other reasons be stored in the public cloud is retained in on-premises datacentres or in a private cloud. Data classification can also enable cloud customers to ensure that the security controls offered by a cloud provider matches the sensitivity of the data stored in the cloud.

Data classification processes vary depending on the organisation's datasets, processing capabilities and how the data is transmitted throughout the organisation, but the objective is to find a method of categorising the organisation's information assets that fits within the organisation's business, organisational and legal requirements. According to the ISO/IEC 17799:2005 standard, "information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization." This can be translated into requirements to identify the level of confidentiality of the data, the privacy impact of the data, the legal and regulatory requirements that apply to the handling of the data, and the business impact of the data. In this respect, Microsoft can assist organisations to classify and manage their information, through solutions such as the File Classification Infrastructure (FCI) technology and the Data Classification Toolkit.

An effective data classification process also ensures that information assets are adequately protected based on their classification by dictating the minimum security controls that must be deployed when handling a particular information asset. As a rule, the higher the value of the dataset, the tighter the security controls applying to such dataset should be. Again, Microsoft offers a range of services, products and technologies that help organisations to ensure that appropriate security controls are implemented to protect their data, such as Data Loss Prevention (DLP) and Microsoft Active Directory Right Management Services (AD RMS).

For more information about data classification and Microsoft services, products and technologies to consider to implement an appropriate information classification and enforcement infrastructure, please see "Protect and control your key information assets through information classification", available at: http://www.microsoft.com/en-us/download/details.aspx?id=44565.

International Standards

There are a number of international standards that are helpful when cloud customers and providers embark upon developing data classification and risk assessment and management strategies for information security management. In particular:

- ISO 27001 provides a global benchmark for identifying overall information security risks and deciding on controls to address them.
- ISO 27018 — a new cloud-specific standard — provides guidance to cloud service providers for assessment of risks and implementation of state-of-the art controls for protection of personal data stored in the cloud. Cloud service providers that adopt ISO 27018 must, among other obligations:
    - process personal data pursuant to the instructions of the cloud customer;
    - refrain from processing such personal data for advertising and marketing purposes without the cloud customer's express instructions;
    - be transparent with their customers about the location of their data; and
    - notify customers of any security breach affecting the customers' personal data in the cloud.

A cloud service provider's audited compliance with the controls in ISO 27001 and 27018 gives organisations an easy way to confirm that the personal data entrusted to the cloud will be kept secure and processed in compliance with their instructions.

Traditional Security Risks

Every year, despite mandated privacy and security regulations, a significant number of data security breaches occur. For example, in the UK alone, there were 701 reported data breaches affecting the health sector in 2013 and 2014.

A recent set of Ponemon Institute reports, "Cost of Data Breach", looks at data breaches in the UK, France, Italy and Germany. The reports examine the causes of data breach and conclude that in all markets a significant proportion of security incidents affecting data are attributable to negligence and human error. For example, in the UK, 40% of data breaches involved mis-steps by employees or contractors. The reports also conclude that lost or stolen devices (including mobile devices such as smart phones and tablets) increase the per capita cost of a data breach between €7 and €15 depending on the market.

Similarly, a recent study by the Center for Media, Data and Society, "Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005-2014", concludes that over half (57%) of all studied data breaches involve organisational errors, insider abuse or theft, or other internal mismanagement (i.e., data being exposed online or mismanaged in an organisational accident, such as lost or stolen hardware or administrative errors).

The Ponemon reports further conclude that in most markets, the cost of data breaches rose during 2013, and on average the total costs incurred by organisations ranged between €1.93 and 3.42 million. The reports also find that organisations experience an increase in customer turnover following a data breach, involving reputational harm and diminished goodwill. In the UK, the cost of lost business as a result of a data breach has been on the increase since 2008.

These scenarios provide only examples of the myriad health security risks that an organisation can face, and illustrates the importance of managing these risks within an effective Health Risk Management Framework.

Cloud-related Risks and Opportunities: Key Questions for Health Organisations to Consider

The shift to cloud computing offers health organisations enormous efficiencies, allowing far greater flexibility and capital cost reductions, while most importantly improving provider and patient access to real-time information. However, this shift often changes the way that organisations operate, and presents challenges to DPOs and information security professionals.

Among the privacy and security-focused questions organisations should ask are:

- Has an effective data classification and governance procedure been implemented to identify sensitive information and to apply the correct level of control for maintaining the security and privacy of the information? If not, what are the required steps to establish this procedure?
- What rights does the cloud service provider reserve over customer data stored in the cloud? In particular, will the cloud service provider use sensitive health information stored in the cloud for its own independent purposes, such as advertising and marketing?
- Who is ensuring data integrity for the computer systems? Are these systems stable?
- Do the cloud computer systems implement any data encryption mechanisms for data-in-transit or for data-at-rest?
- Does the security architecture of such systems comply with industry standards?
- Does the cloud service provider offer comprehensive and easy-to-understand information about its privacy and security practises?
- What assurances does the cloud service provider offer regarding the handling of law enforcement requests to access data stored in the cloud?
- What happens to the data after the cloud service comes to an end? In particular, is the customer data securely deleted after expiration of the cloud contract?
- What measures does the cloud service provider use to safeguard personal data transferred outside the EEA (e.g., Safe Harbor, European Commission's Model Clauses, binding corporate rules)?

These are just a few of the questions that DPOs and IT security professionals need to ask as they develop a data protection and security strategy for their cloud environment.

Before cloud computing technologies emerged, many of these inherent security and privacy risks existed in traditional (non-cloud-based) computing environments. However, since the boundaries of a traditional computing environment typically existed within the scope of an organisation's IT structure, organisations had greater control of management of such risks. With the introduction of cloud technologies, risk management responsibility is no longer confined to the internal IT organisation. In this environment, health organisations may find it challenging to understand the scope of their responsibility across the enterprise and beyond. Understanding this new playing field and the players is very important to managing risk. In a traditional computing environment, the risk existed but it was fully owned by the organisation in the health sector. In a cloud-based scenario, the equation changes from a single risk owner to shared risk ownership between the cloud service provider and the cloud customer.

As part of its online services, Microsoft has developed a contractual framework to address this challenge. This framework consists of

a comprehensive data processing agreement, which is accompanied by the EU "Model Clauses". The Model Clauses are provisions adopted by the Commission that, where implemented, enable the lawful transfer of personal data outside of the EEA. Significantly, the Article 29 Working Party and the DPAs of Luxembourg, the Czech Republic and Spain have concluded that Microsoft's Model Clauses meet the requirements set out in the EU's Data Protection Directive 95/46/EC. Microsoft's contractual commitment to comply with the Model Clauses gives its customers reassurance that their sensitive health data will always be processed in compliance with EU data protection laws. A copy of the Article 29 Working Party letter approving Microsoft's Model Clauses is provided in Appendix A to this White Paper.

The contractual framework offered by Microsoft to its cloud customers is an effective solution to facilitate shared risk ownership between the customer and the cloud service provider, resulting in a successful Shared Risk Strategy. Effective utilisation of a Health Risk Management Framework and having a Shared Risk Strategy will enable organisations to not only mitigate traditional risks, but also to more successfully adopt new cloud-based models.

Trustworthy Computing: Microsoft's Approach to End-to-End Trust

Microsoft is committed to building software and services that help protect our customers and the industry. Our approach to security includes both technological and social aspects, and we strive to ensure that information and data are safe and confidential.

The End-to-End Trust approach to security and privacy is part of a comprehensive vision for a trustworthy Internet ecosystem, one that enables everyone to make effective trust decisions about their health information.

Figure 3: Trustworthy Computing (End-to-End Trust)

Trusted People – Identity-based access combined with encryption, certification, and authentication enhances control of access to confidential data, documents and care records.

Trusted Devices – Designed by applying a holistic approach to security, Windows 8 and Windows Phone offer health workers their choice of feature-rich, flexible devices.

Trusted Operating System (OS) – The Secure Boot, a new security feature in Windows 8, blocks the loading of any program that has not been signed by an OS-provided key, helping protect the integrity of devices, system files, and software.

Trusted Software and Applications – A .NET-based application platform protects patient data using built-in cryptology, centrally managed apps, and cloud-ready corporate authentication services.

Trusted Data – With Information Rights Management, health workers can restrict document permissions for specific people, helping prevent personal health information (PHI) from falling into the wrong hands.

Delivering on End-to-End Trust requires management of identity and access, and applying audit controls across a trusted stack of people, devices, operating system, application software and data.

Microsoft delivers End-to-End Trust across on-premises, cloud and hybrid scenarios. Addressing health regulations is

embedded in the DNA of Microsoft's cloud solutions. With Microsoft solutions, health organisations can consolidate on one cloud, with one infrastructure partner and with a common security and privacy framework that is specifically tailored to help address the compliance needs of health-covered entities.

Health Risk Management Framework

The Health Risk Management Framework provides an effective and continuous approach model inspired by the ISO/IEC 27001 – Plan, Do, Check, Act cycle. This framework focuses primarily on risk management and incorporates several industry best practises to bring an effective framework for managing health risk. It has four phases.

1. Identify – Identify the organisational assets, classify them and provide relative rank of the organisational assets.
2. Assess – Assess the threats and vulnerabilities associated with those assets using qualitative and quantitative approach.
3. Implement – Once the assessment is complete, deploy and implement control solutions to reduce risk to the business.
4. Monitor – Monitor the risk management process for effectiveness and re-affirm if the controls are providing the expected degree of protection.

Figure 4 below illustrates the four phases of the Health Security Risk Management Process.

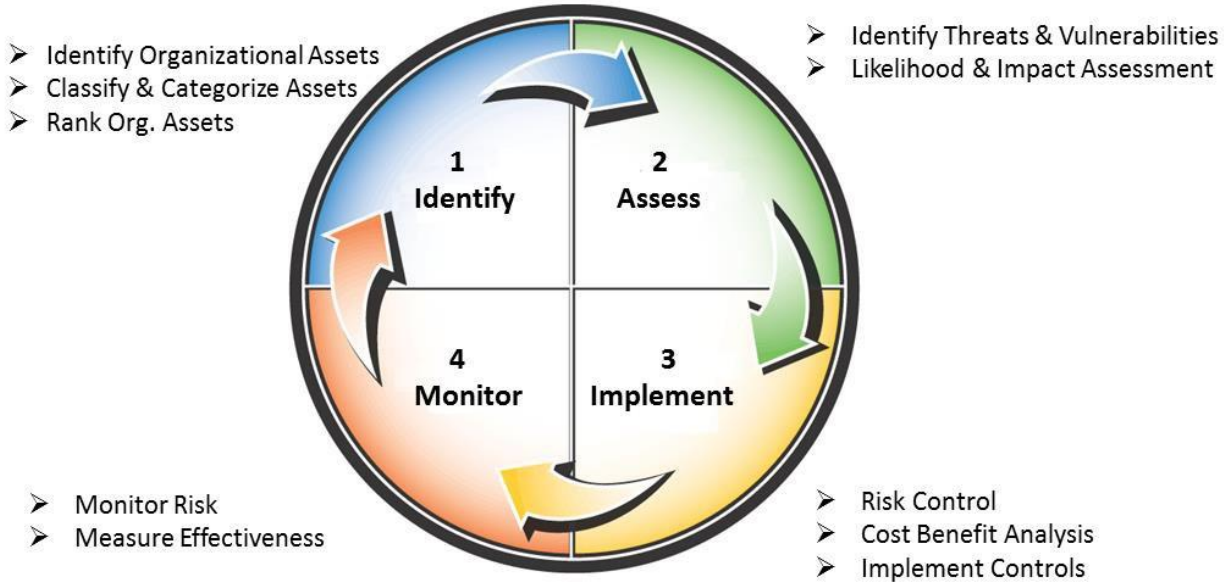


Figure 4: Health Risk Management Framework

1. Identify

Identify is the process of self-analysis. Here, the security team analyses the organisational assets and classifies them into various

categories to rank/prioritise them by their relative importance.

Organisational Assets Inventory

One of the important steps of asset identification is to take into account what assets the organisation currently has. Many organisations tend to assume that an organisational asset is something that is only tangible. This is not correct. Organisational asset is anything that is of business value to the organisation – this includes tangible and non- tangible assets such as people, processes, data, software, hardware and network components. An asset can be uniquely identified using their name, tags and serial number, etc.

Once the ranking is completed, the next step is to evaluate the systems for various threats & vulnerabilities.

2. Assess

Risk Assessment is an important step which measures risk in numeric terms. In order to perform risk assessment we should understand two important terms – Vulnerability and Threat.

Vulnerability and Threat

In simple terms, a flaw or weakness in an organisational asset that could be exploited is termed as vulnerability.

Threat is an action triggered by a threat source to exploit a specific vulnerability.

In order to assess the risk of threats it is imperative to understand the vulnerabilities associated with various organisational assets and also understand the potential threats that could exploit the identified vulnerabilities. Security Team can identify a list of threat-sources. Threat sources could be classified as Natural Threats (e.g., flood), Human Threats (e.g., Hackers), and Environmental Threats (e.g., Chemicals). Once the threat sources are identified, the next step is to list the motivation for the threat source to act. This combination will help us identify a threat action. For example if the threat source is an "Internal Employee" and the motivation is "Revenge", then the possible threats are "Assault of an employee", "System & Data abuse", "Data Theft" and "System Sabotage".

This approach can be used to identify all the threats in an organisation. Identifying vulnerability is a more collective effort involving various groups – technical team, business team, finance team etc. It is necessary to collect the vulnerability from every aspect and not fall into the trap of focusing on technical vulnerabilities alone.

Once the vulnerabilities and associated threats are identified, the next step is to assess the potential business impact in terms of quantity and quality.

3. Implement

Once the risk assessment is complete, the next step is to select and implement the controls. But before the controls can be implemented it is necessary to understand that every risk control used falls under one of the Risk Control Strategies defined below.

- Avoid: Apply measures to eliminate the risks

- Transfer: Shifting the risks to some outside an entity
- Mitigate: Reducing the impact of a possible risk after it occurs
- Accept: Understanding the consequences and accepting the risk without any attempt to act on that risk. Hence, this strategy has no controls.

Below are some of the risk controls that fall under various Risk Control Strategies.

Avoidance Controls

Many controls can be implemented to avoid risks. For example:

- Education & Training: Education and training would be a proper avoidance control for various social engineering attacks such as Phishing, Spear Phishing, etc.
- Technology Control: Implementing the right technology solution like firewall could prevent an attack such as Ping of Death.

Transfer Controls

Transferring the implications of a risk is definitely a consideration when the impact of the risk is primarily monetary. For example:

- Insurance: Insuring against a risk is a form of risk transfer. In the event of a risk turning into an actual event, the monetary impact is transferred to the insurance company.
- Sourcing: The maintenance of the network could be sourced to a third party and the monetary and legal risks could be transferred to the sourcing organisation.

Mitigation Controls

Mitigation is the most commonly used risk mitigating strategy. Reducing the impact of a potential risk is achieved by implementing controls. For example:

- A fire extinguisher setup in data centres, biometric locks, Disaster Recovery (DR), Business Continuity (BC), Antivirus for organisational devices, etc. are various forms of mitigation strategies that could be implemented.
- DR, BC and Incident Response (IR) are key mitigation strategy controls that every organisation should create and plan for, as it is critical for the sustenance of the organisation.

Cost Benefit Analysis

Before these controls can be implemented it is necessary to perform a Cost Benefit analysis to understand if the cost of implementing the controls is worth the risk.

Once the risk control measures are implemented it is necessary to constantly monitor and make necessary adjustments to stay updated. The details of this are explained in the final phase of the framework.

4. Monitor

Change is an inevitable and integral part of an organisation which helps it to progress. Implementing a control strategy does not mean that risks are mitigated because a change brings with it new challenges. Hence, it's necessary to periodically review and

evaluate the control strategies as the organisation evolves. An ideal scenario would be to review it every one month to ensure high degree of compliance and security. Below are some of the steps that organisations can take to monitor and manage risk controls:

- Create and review metrics associated with all implemented security risks and controls
- Assess the effectiveness of implemented controls
- Check adherence to compliance mechanisms applicable for the organisation
- Update IT assets and security risks as needed
- Conduct periodic third party security assessments and reviews
- Perform vulnerability and penetration testing

Additionally, encouraging employees to provide constant feedback and controlling organisational assets using a compliance mechanism would enable organisations to stay up-to-date and make sure that the organisation's risk is managed successfully.

Shared Risk Strategy in European Health Sector

Shared Risk Strategy is pivotal to effectively managing risks when health organisations are using cloud-based solutions. Let's review Microsoft's Data Processing Agreement (with EU Model Clauses) and related compliance framework for Microsoft Online Services and understand what Shared Responsibility is all about.

Microsoft's Data Processing Agreement (with EU Model Clauses)

Microsoft recognises that data security and patient privacy are fundamental requirements across the health industry, and Microsoft takes its role very seriously. This is why Microsoft provides all its customers a comprehensive data processing agreement with the EU Model Clauses that together address the privacy and security of customers' data in the cloud.

The compliance framework for Microsoft Online Services, including the Model Clauses, ensures that Microsoft meets the highest data protection and security safeguards. Among Microsoft's commitments:

- Microsoft does not use its customers' data for its own commercial purposes, such as to deliver targeted advertising. Health organisations retain control of their sensitive data at all times.
- Microsoft does not provide any government with direct, unfettered access to customers' data. Microsoft ensures that only authorised individuals will have access to data in the cloud.
- Microsoft online services and data centres are designed to enable the physical, administrative, and technical safeguards to assist health organisations with their compliance requirements. In particular, Microsoft assists its customers to comply with their notification obligations in the event of a data breach by committing to inform customers of such breaches.
- Microsoft data centres are SAS 70 Type II, and ISO 27001 certified, and are audited by independent, third-party security organisations.
- Microsoft is committed to deleting customer data no more than 180 days after expiration or termination of customer's use of the online services.
- Microsoft provides comprehensive information about the location of its data centres via online data maps and provides notice to customers if there are changes to those maps. Customer's country or region determines the primary storage location for the customer's data.

With Microsoft's agreements and compliance with industry governing bodies, Microsoft enables its customers to continue to meet their mandated compliance needs, whether in the cloud or on premise.

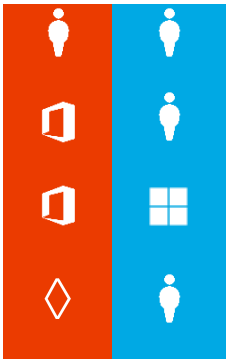
Shared Responsibility: Privacy and Security Matrix

Shared responsibility for privacy and security compliance in the cloud is inevitable and it is advocated by Microsoft. Understanding what "shared responsibility" means in practice is important to the success of effective risk management and compliance.

The Privacy and Security Matrix below illustrates the shared responsibility between the vendor (cloud service provider) and the cloud customer to achieve the highest levels of compliance. The Matrix goes through some of the most important privacy and security controls arising from the EU data protection laws and outlines the ownership associated with the controls when using Windows Azure & Office 365.

In the Matrix, the responsibilities for privacy and security safeguards belong either exclusively to the cloud service provider, the customer, or they are shared between the parties. In addition, some of the safeguards are the responsibility of the customer but the cloud service provider is required to assist the customer to implement the control, e.g., by providing information about the IT infrastructure of the cloud service provider. The Matrix should be read with the help of the following key:

Key



Responsibility of the customer

Responsibility is shared

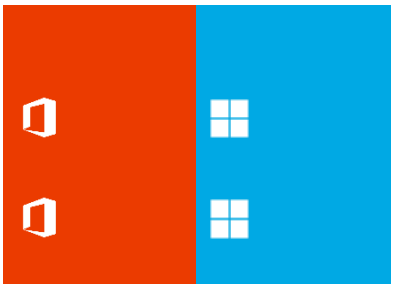
Responsibility of the cloud service/platform

Responsibility of the customer but contribution from cloud service/platform

Health organisations considering the adoption of cloud services should use the Matrix as a tool in developing their risk assessment and information management framework. Microsoft encourages a constructive dialogue with its customers and partners regarding the Matrix, which provides a joint opportunity to accelerate the adoption of cloud services in the health sector.

Data Processing Requirements*

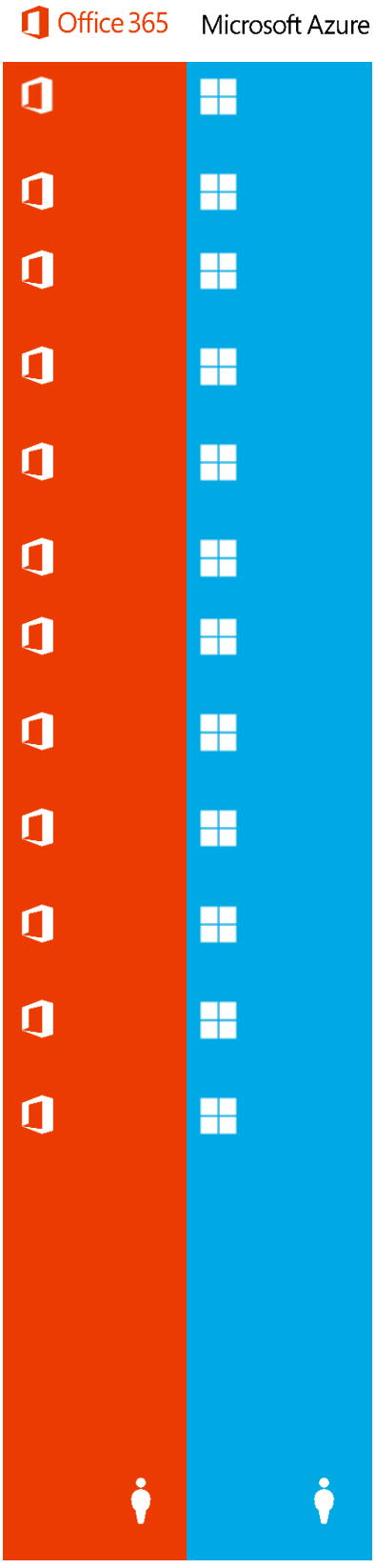
Office 365 Microsoft Azure



1. Cloud service provider only processes personal data under instructions from the cloud customer
2. Cloud service provider implements technical and organisational security measures that adequately protect personal data

3. Cloud service provider commits that it and its employees will keep personal data confidential and only authorised persons will have access to the information
4. Cloud service provider promptly reports security incidents to cloud customer
5. Cloud service provider promptly notifies the cloud customer about any legally binding request for disclosure by law enforcement agencies
6. Cloud service provider promptly notifies the cloud customer about data subject access requests
7. Cloud service provider provides a list of locations in which personal data may be processed
8. Cloud service provider deals with customer inquiries promptly
9. Cloud service provider submits its processing facilities for audit if requested by cloud customer
10. Cloud service provider obtains cloud customer's prior consent to the use of sub-processors and notifies the cloud customer if there are changes to those sub-processors
11. Cloud service provider enters into a written agreement with sub-processors that requires the sub-processor to comply with the same obligations as the cloud service provider
12. Cloud service provider keeps a list of all sub-processing agreements and sends promptly a copy of any such sub-processing agreement to the cloud customer if requested
13. Cloud service provider ensures that any cross-border transfer of personal data to sub-processors is carried out in accordance with the EU Data Protection Directive
14. Cloud service provider returns or securely erases personal data after termination of the cloud services

* These requirements are typically imposed on the cloud service provider via the data processing contract and/or the EU Model Clauses



Administrative Safeguards

Security Management Process

1. Identify and classify relevant information systems and personal data stored in those systems

2. Conduct risk assessment
3. Implement a risk management program
4. Acquire IT systems and services
5. Create and deploy policies and procedures
6. Develop and implement a sanction policy
7. Develop and deploy an information system activity review process
8. Develop appropriate standard operating procedures
9. Implement the information system activity review and audit process

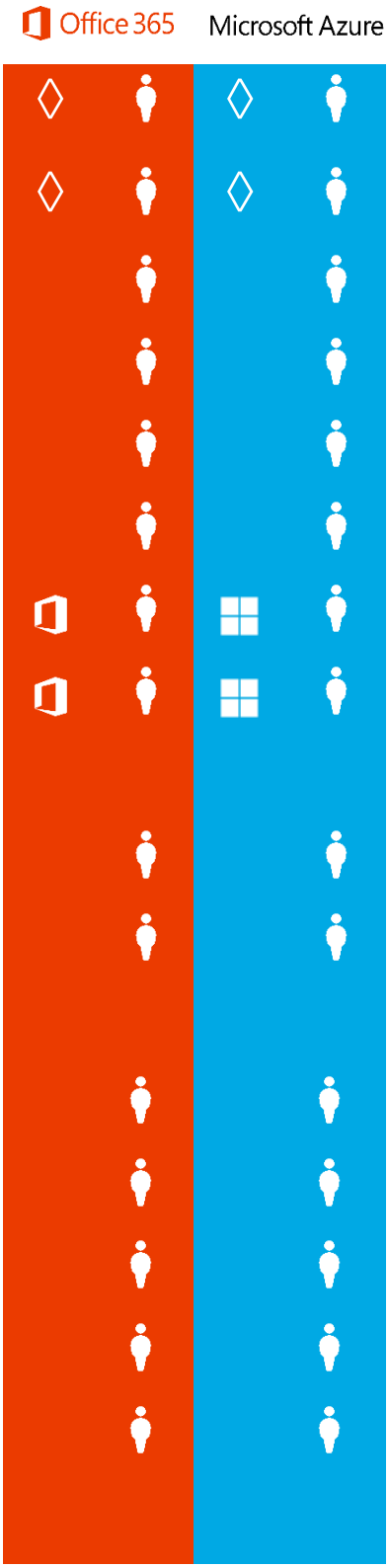
Assigned Security Responsibility

1. Select an official to be assigned responsibility for data privacy and security
2. Assign and document the individual's responsibility

Workforce Security

1. Implement procedures for authorisation and/or supervision
2. Establish clear job descriptions and responsibilities
3. Establish criteria and procedures for hiring and assigning tasks
4. Establish a workforce clearance procedure
5. Establish termination procedures

Information Access Management



1. Implement policies and procedures for authorising access
2. Implement policies and procedures for access establishment and modification
3. Evaluate existing security measures related to access controls

Security Awareness and Training

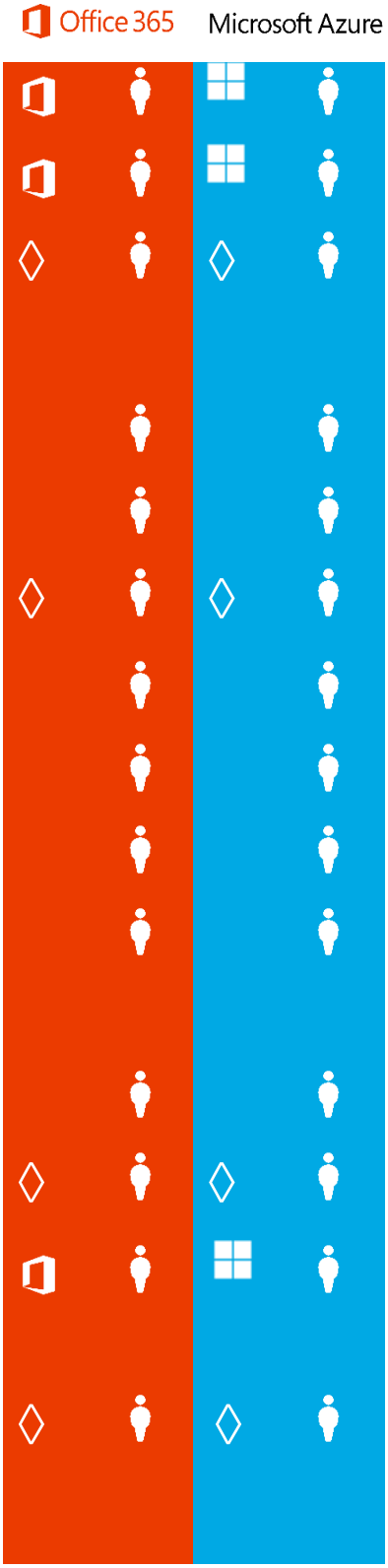
1. Conduct a training needs assessment
2. Develop and approve a training strategy and a plan
3. Protection from malicious software; log-in monitoring; and password management
4. Develop appropriate awareness and training content, materials, and methods
5. Implement the training
6. Implement security reminders
7. Monitor and evaluate training plan

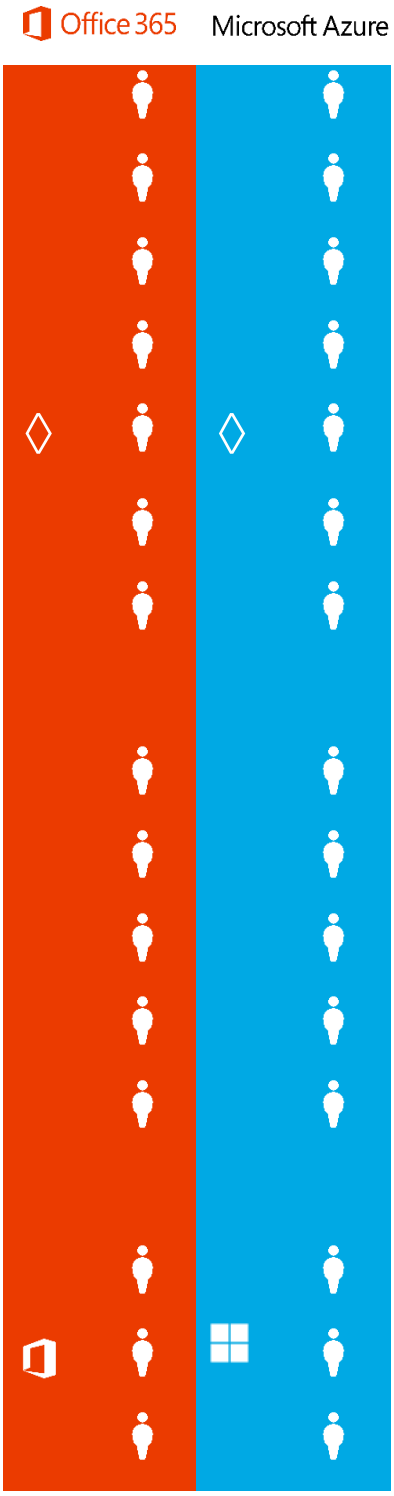
Security Incident Procedures

1. Determine goals of incident response
2. Develop and deploy an incident response team or other reasonable and appropriate response mechanism
3. Develop and implement procedures to respond to and report security incidents*

   * While the cloud customer is legally responsible for responding to and reporting security incidents, in practice cloud service providers are contractually required to provide notification to cloud customers of security incidens
4. Incorporate post-incident analysis into updates and revisions

Contingency Plan





1. Develop contingency planning policy
2. Conduct an applications and data criticality analysis
3. Identify preventive measures
4. Develop recovery strategy
5. Data backup plan and disaster recovery plan
6. Develop and implement an emergency mode operation plan
7. Testing and revision procedure

Evaluation

1. Determine whether internal or external evaluation is most appropriate
2. Develop standards and measurements for reviewing all standards
3. Conduct evaluation
4. Document results
5. Repeat evaluations periodically

Data Processing Contracts and Other Arrangements

1. Identify entities acting as data processors under the EU data protection framework
2. Written contract or other similar arrangement
3. Establish process for measuring contract performance and terminating the contract if data protection and security requirements are not being met

Physical Safeguards

Facility Access Controls

1. Conduct an analysis of existing physical security vulnerabilities
2. Identify corrective measures
3. Develop a facility security plan
4. Develop access control and validation procedures
5. Establish contingency operations procedures
6. Maintain maintenance records

Workstation Use

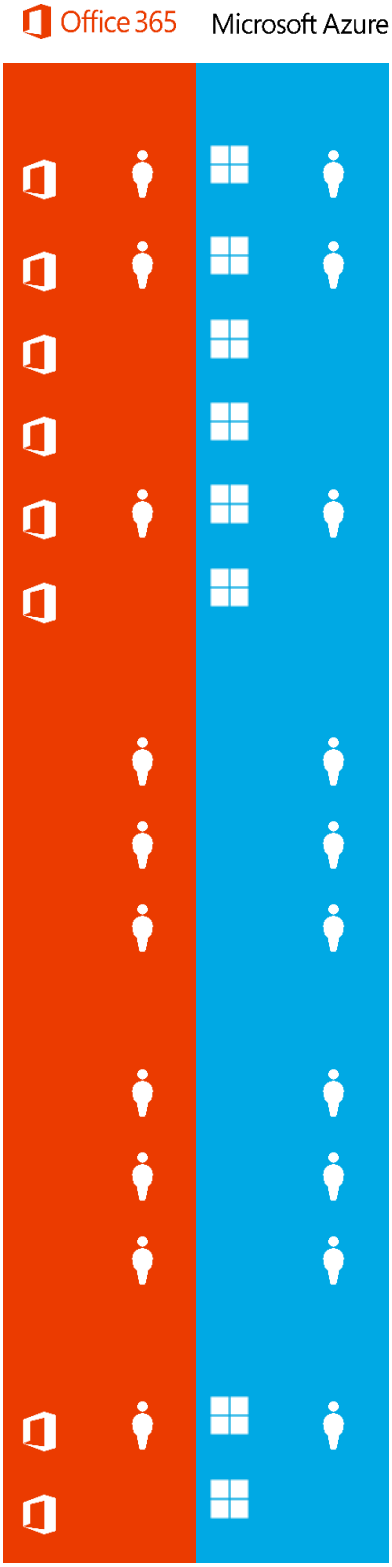
1. Identify workstation types and functions or uses
2. Identify expected performance of each type of workstation
3. Analyse physical surroundings for physical attributes

Workstation Security

1. Identify all methods of physical access to workstations
2. Analyse the risk associated with each type of access
3. Identify and implement physical safeguards for workstations

Device and Media Controls

1. Implement methods for final disposal of electronic personal data
2. Develop and implement procedures for reuse of electronic media



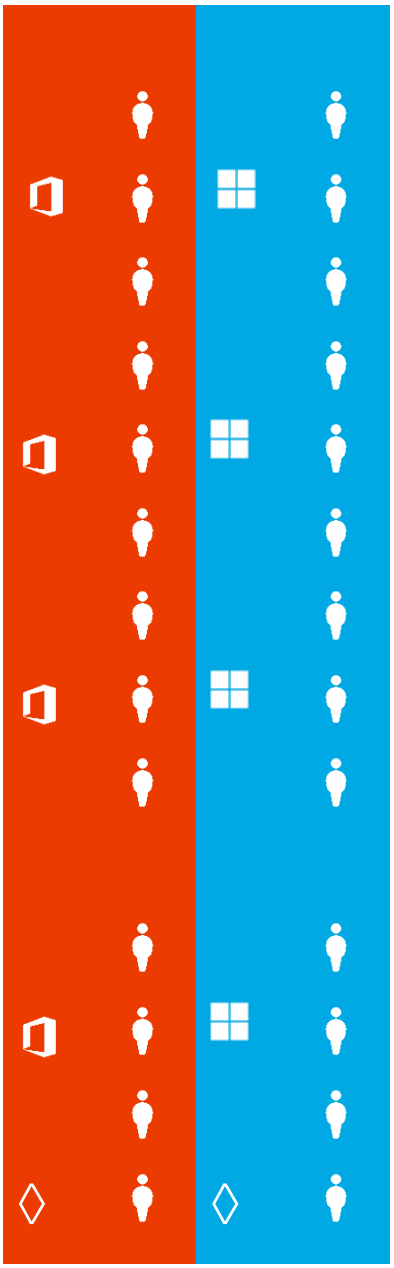
3. Maintain accountability for hardware and electronic media

4. Develop data backup and storage procedures

Technical Safeguards

Access Control

1. Analyse workloads and operations to identify the access needs of all users
2. Identify technical access control capabilities
3. Ensure that all system users have been assigned a unique identifier
4. Develop access control policy
5. Implement access control procedures using selected hardware and software
6. Review and update user access
7. Establish an emergency access procedure
8. Automatic logoff and encryption and decryption
9. Terminate access if it is no longer required



Audit Controls

1. Determine the activities that will be tracked or audited
2. Select the tools that will be deployed for auditing and system activity reviews
3. Develop and deploy the information system activity review/audit policy
4. Develop appropriate standard operating procedures

5. Implement the audit/system activity review process

Integrity

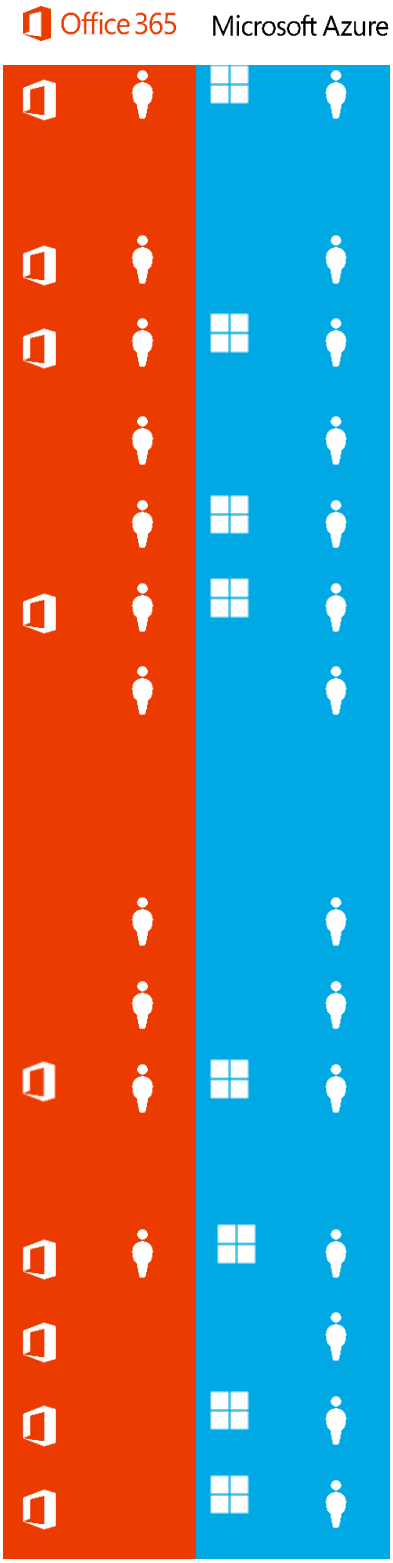
1. Identify all users who have been authorised to access personal data
2. Identify any possible unauthorised sources that may be able to intercept the information and modify it
3. Develop the integrity policy and requirements
4. Implement procedures to address these requirements
5. Implement a mechanism to authenticate personal data
6. Establish a monitoring process to assess how the implemented process is working

Person or Entity Authentication

1. Determine authentication applicability to current systems/applications
2. Evaluate authentication options available
3. Select and implement authentication option

Transmission Security

1. Identify any possible unauthorised sources that may be able to intercept and/or modify the information
2. Develop and implement transmission security policy and procedures
3. Implement integrity controls
4. Implement encryption



Data Retention and Deletion

1. Identify data retention periods to ensure personal data is not retained longer than necessary for the purpose for which it was collected
2. Ensure secure deletion of personal data at the end of retention period, e.g., via overwriting

Organisational Requirements

Data Processing and Transfer Contracts

1. Put in place a written data processing agreement between the cloud customer and the cloud service provider
2. Ensure any cross-border transfer of personal data is carried out in accordance with the EU Data Protection Directive, e.g., via EU Model Clauses

Policies and Procedures

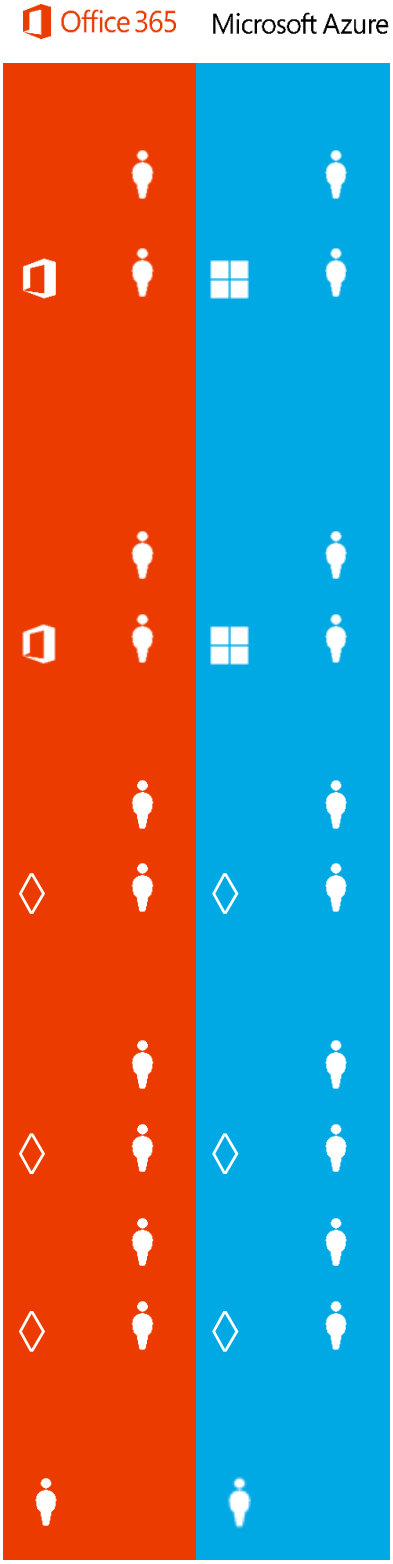
1. Create and deploy policies and procedures
2. Update documentation of policy and procedures

Documentation

1. Draft, maintain and update required documentation
2. Retain documentation for minimum requirements under applicable local laws
3. Assure that documentation is available to those responsible for implementation
4. Update documentation as required

Transparency

1. Take appropriate steps to inform individuals about the processing of their personal data in the cloud



Health Moving to the Cloud

Health organisations are finding it increasingly difficult to accomplish the triple aim of effective healthcare:

- improving quality of care;
- providing better access to care for an increasing number of patients; and
- lowering the cost of care (while maintaining high quality of and better access to care).

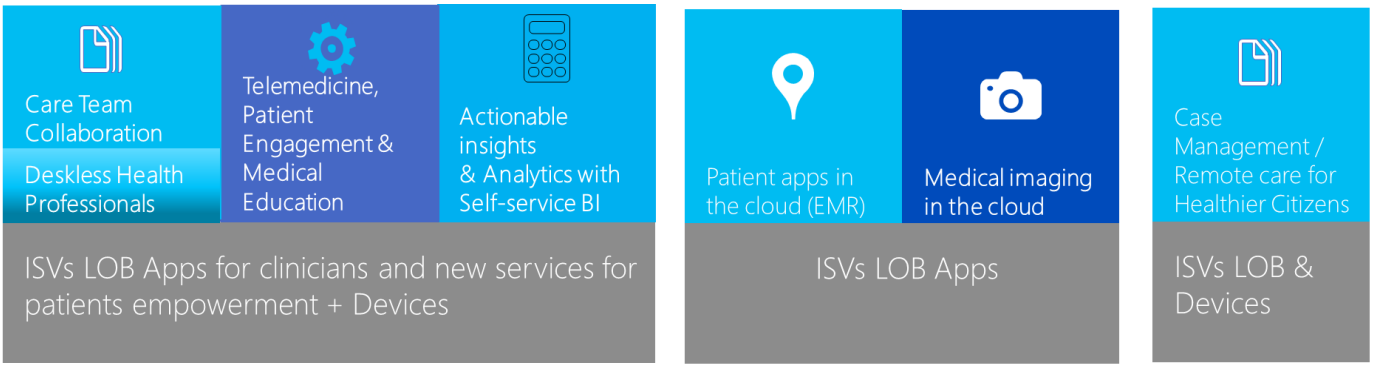


Figure 5 Health Moving to the Cloud: O365, Microsoft Azure, Dynamics CRM Online

More and more health organisations are turning to the cloud to improve effeciencies and take advantage of innovations. It is important to remember that cloud adoption is not an all or nothing proposition, and instead, health organisations around the world are adopting both hybrid-cloud as well as pure-cloud solutions. Areas where cloud services have been adopted in the health sector include:

Line of Business Applications for Clinicians and New Services for Patient Empowerment:

- Care Team Coordination
- Deskless Health Professionals
- Telemedicine
- Patient Engagement
- Continued Medical Education
- Actionable Insights and Analytics with Self-Service Business Intelligence

Line of Business Applications build by Independent Software Vendors (ISVs)

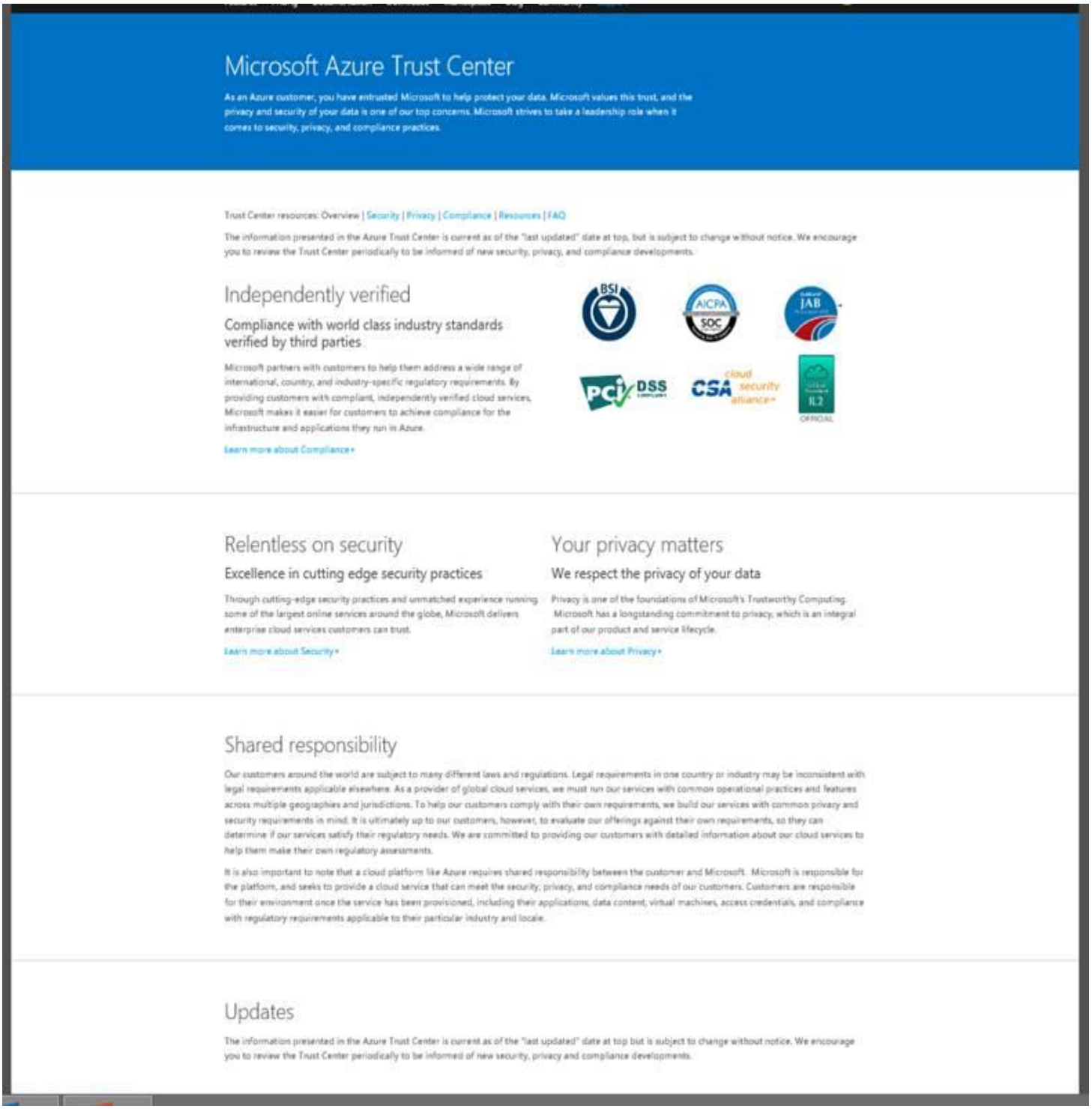
- Patient Applications in the Cloud (EMR)
- Medical Images in the Cloud

Line of Business Applications for Devices/Mobile Solutions

- Care Management and Remote Care for Healthier Citizens

Microsoft Trust Centre

The privacy and security of data is one of Microsoft's top concerns. Microsoft strives to take a leadership role when it comes to security, privacy, and compliance practices. The Microsoft Azure Trust Centre is the location which consolidates details on policies, certifications, attestations and rich resources on privacy, security, and compliance: http://azure.microsoft.com/en-us/support/trust-center/



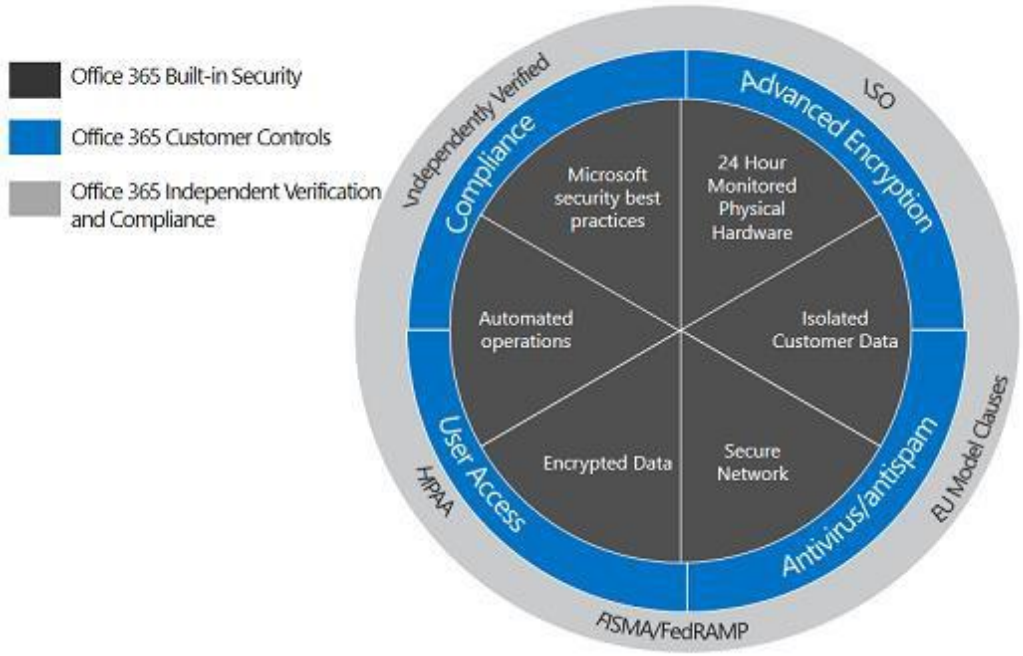
Windows Azure Trust Centre

Program	Description

ISO 27001	• Internationally recognised information security standard that is broadly accepted around the world ,133 controls across 11 domains • Annual surveillance audits with continual improvement
EU Data Protection Directive	• Law that sets a baseline for handling personal data in the EU, Microsoft complies through EU-US Safe Harbor Framework and the EU Model Clauses approved by the Article 29 Working Party
SSAE 16 / ISAE 3402	• Accounting standard relied upon as the authoritative guidance for reporting on service organisations (SOC 1, SOC 2, SOC 3) • Annual audit, controls monitored for 6 months, 10 domains, detailed audit report shared with customers under NDA

O365 Trust Centre

Office 365 has scalable security processes that allow for independent verification and compliance with industry standards.



Operating a global cloud infrastructure creates a need to meet compliance obligations and to pass third-party audits. Auditable requirements come from government and industry mandates, internal policies, and industry best practises. Office 365 ensures that compliance expectations are continuously evaluated and incorporated. As a result, Office 365 has obtained independent verification, including ISO 27001 and SSAE16 SOC 1 (Type II) audits, is able to transfer data outside of the European Union through the U.S.-EU Safe Harbor Framework and the EU Model Clauses, offers a Data Processing Agreement as a default to all customers, and has disclosed security measures through the Cloud Security Alliance's public registry. Office 365 extends the controls implemented to meet these standards to customers who are not necessarily subject to the respective laws or controls.

Certified for ISO 27001

ISO 27001 is one of the best global security benchmarks. Office 365 is the first major business productivity public cloud service to have implemented the rigorous set of physical, logical, process, and management controls defined by ISO 27001.

EU model clauses

In addition to being certified under EU Safe Harbor, Office 365 is the first major business productivity public cloud service provider to sign the standard contractual clauses created by the European Union ("EU model clauses") with all customers as a default. EU model clauses address international transfers of data. Microsoft's EU model clauses have been approved by the Article 29 Working Party, a group consisting of the local data protection authorities of all the EU Member States, as meeting the requirements set out in the EU Data Protection Directive 95/46/EC.

Data processing agreement

At Microsoft, we offer a comprehensive standard data processing agreement (DPA) to all customers as a default. The DPA addresses the privacy, security, and handling of customer data. Our standard data processing agreement enables customers to comply with their local regulations arising from the national laws implementing the EU Data Protection Directive 95/46/EC.

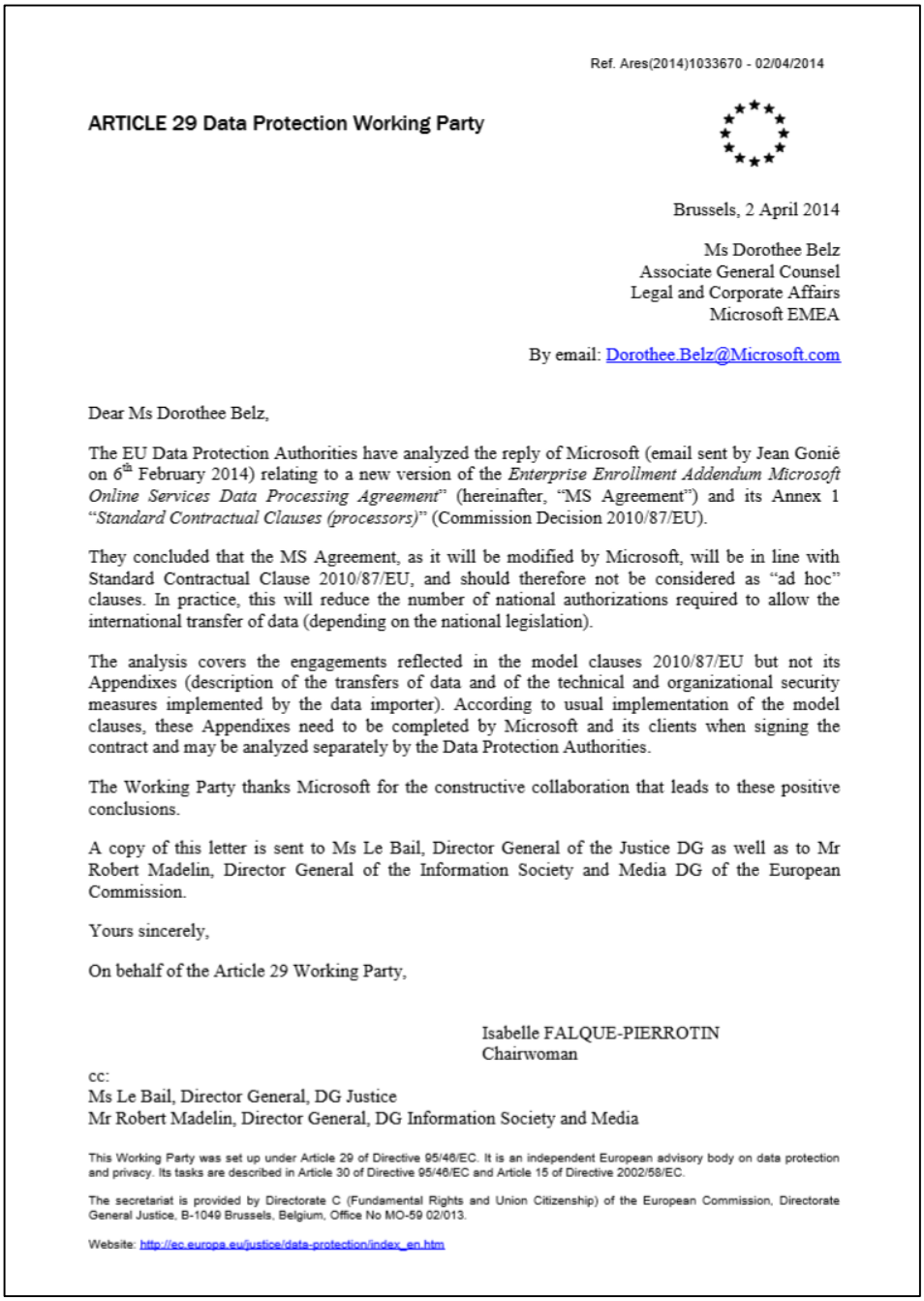
Conclusion

Health organisations wrestle with how to evaluate the security and privacy aspects of the cloud and how these relate to their companies' existing risk profiles. There are benefits and challenges in whether applications and infrastructure are hosted on premise, off-premise or a combination of the two. There are many choices and many risks that go along with each choice and it's important to evaluate what will be optimal for each organisation.

Performing Risk Management as defined both in terms of traditional computing environments and cloud-related environments will allow organisations to successfully manage their risks. Additionally, when organisations purchase new products and services (which diminish the security boundaries of an organisation) it is paramount to evaluate the products and service offerings from a health security perspective.

This paper provides an effective framework for health risk management and discusses the shared risk strategy for cloud services. Organisations utilising this framework and understanding the shared mode of responsibility in a cloud environment will be better positioned to focus on their competitive strategy and take on greater challenges in the future knowing that their risks are well managed.

Appendix A: Article 29 Working Party - Joint Letter



Ref. Ares(2014)1033670 - 02/04/2014

ARTICLE 29 Data Protection Working Party

Brussels, 2 April 2014

Ms Dorothee Belz
Associate General Counsel
Legal and Corporate Affairs
Microsoft EMEA

By email: Dorothee.Belz@Microsoft.com

Dear Ms Dorothee Belz,

The EU Data Protection Authorities have analyzed the reply of Microsoft (email sent by Jean Gonié on 6th February 2014) relating to a new version of the *Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement*" (hereinafter, "MS Agreement") and its Annex 1 "*Standard Contractual Clauses (processors)*" (Commission Decision 2010/87/EU).

They concluded that the MS Agreement, as it will be modified by Microsoft, will be in line with Standard Contractual Clause 2010/87/EU, and should therefore not be considered as "ad hoc" clauses. In practice, this will reduce the number of national authorizations required to allow the international transfer of data (depending on the national legislation).

The analysis covers the engagements reflected in the model clauses 2010/87/EU but not its Appendixes (description of the transfers of data and of the technical and organizational security measures implemented by the data importer). According to usual implementation of the model clauses, these Appendixes need to be completed by Microsoft and its clients when signing the contract and may be analyzed separately by the Data Protection Authorities.

The Working Party thanks Microsoft for the constructive collaboration that leads to these positive conclusions.

A copy of this letter is sent to Ms Le Bail, Director General of the Justice DG as well as to Mr Robert Madelin, Director General of the Information Society and Media DG of the European Commission.

Yours sincerely,

On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN
Chairwoman

cc:
Ms Le Bail, Director General, DG Justice
Mr Robert Madelin, Director General, DG Information Society and Media

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

References & Further Reading

- Windows Azure Business Continuity Technical Guidance
  - http://msdn.microsoft.com/en-us/library/windowsazure/hh873027.aspx
- Windows Azure Trust Center – Security
  - http://www.windowsazure.com/en-us/support/trust-center/security/
- Office 365 Security Whitepaper
  - http://office.microsoft.com/en-us/business/redir/XT104030898.aspx
- Office 365 Enterprise
  - http://office.microsoft.com/en-us/business/office-365-enterprise-e3-business-software-FX103030346.aspx
- Office 365 Security
  - http://office.microsoft.com/en-us/business/microsoft-business-security-solutions-FX103045813.aspx
- Security, Privacy and Compliance Information for Office 365
  - http://www.microsoft.com/online/legal/v2/?docid=27
- Addressing Cloud Computing Security Considerations with Microsoft Office 365
  - http://download.microsoft.com/download/2/2/0/220AE513-4A01-4D95-9275-11E71215A0C2/CloudSecurityConsiderations_MicrosoftOffice365.pdf
- Office 365 mapping of CSA Security, Compliance and Privacy Cloud Control Matrix requirements
  - http://www.microsoft.com/en-us/download/details.aspx?id=26647
- Office 365 Enterprise Advanced Privacy Options for Administrators
  - http://www.microsoft.com/online/legal/v2/en-us/E.EDU.GOV_Advanced_Privacy_Options_for_Admins.htm
- Security Risk Management Guide
  - http://technet.microsoft.com/en-us/library/cc163143.aspx
- http://www.windowsazure.com/en-us/support/trust-center/security/
- http://www.windowsazure.com/en-us/support/legal/security-overview/
- http://technet.microsoft.com/en-us/magazine/gg607453.aspx
- http://technet.microsoft.com/en-us/magazine/hh750397.aspx
- http://blogs.technet.com/b/privatecloud/archive/2013/12/06/windows-azure-pack-installing-amp-configuring-series.aspx
- http://www.windowsazure.com/en-us/support/trust-center/privacy/