FOLEY HOAG LLP

Understanding ISO 27018 and Preparing for the Modern Era of Cloud Security

Presented by Microsoft and Foley Hoag LLP's Privacy and Data Security Practice Group
May 14, 2015

FOLEY HOAG LLP

Speakers

- **Sharon Gillett**, Principal Networking Policy Strategist, Microsoft Research
- **Deborah Hurley**, Founder and Principal, Hurley, and Fellow, Institute for Quantitative Social Science, Harvard University
- **Colin Zick**, Partner, Co-Chair and Co-Founder, Privacy & Data Security Practice, Foley Hoag LLP

FOLEY HOAG LLP

Overview

- What are the key data privacy and data protection issues companies should consider before moving to cloud computing technologies?
- What are the key substantive requirements of ISO 27018 for handling customer data?
- How does ISO 27018 adoption benefit customers in regulated industries such as healthcare and financial services?
- How do the ISO 27018 requirements map against existing sector-based data privacy and security standards (e.g., HIPAA, SOC 2)?
- What value is provided by third party verification (through accreditation) of ISO 27018 and other data privacy and security practices in cloud computing?

What is ISO 27018?

- On July 30 2014, the International Organization for Standardization (ISO) adopted ISO 27018 as a voluntary international standard.
  - ISO 27018 governs the processing of personal information by public Cloud Service Providers (CSPs).
- Even though this standard is voluntary, it is widely expected to become the benchmark for CSPs going forward.
- As the first and only international privacy standard for the cloud, ISO 27018 incorporates controls for personally identifiable information (PII).
- ISO 27018 establishes control objectives, controls and guidelines for implementing measures to protect PII.

Meet the ISO 27000 “Family”

- The ISO 27000 family of standards addresses privacy, confidentiality and technical security issues and have:

  "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization." The standards outline hundreds of potential controls and control mechanisms.

- ISO 27001:
  - one of the most widely recognized certifications for a cloud service
  - defines how to implement, monitor, maintain, and continually improve the information security management system (ISMS).
- An organization may obtain an ISO 27001 certification on its ISMS, which is typically based on the ISO 27002 Information Security Standards.

FOLEY HOAG LLP

What are the key data privacy and data protection issues companies should consider before moving to cloud computing technologies?

What privacy and data protection issues should be considered before moving to the cloud?

- Are we dealing with PII, or data that we or our customers would consider sensitive even if not formally classified as PII?
- Does my organization have the resources and know-how to comply on its own? Even if it does, is cloud compliance the highest and best use of my organization's resources?
- Will a cloud provider follow best practices to ensure the security of our data, both in terms of physical security and information access?
- Will the data need to cross borders? Many jurisdictions have stronger data protection laws than the U.S. – can moving our data to the cloud help us with compliance?
- How much transparency and control will we get over what the cloud provider does with our data?
- Will we be able to verify the data protection assurances and contractual commitments we receive from a cloud provider?

What kind of data is it?

- Is it statutorily protected data of any type?
  - Financial
  - Consumer
  - Health care
  - Defense
- IP/Trade Secrets
- Contractually protected:
  - Are the contractual limitations on where data can go or how it is to be protected?

Where is the data?

- It is easy to wind up with data all around the world.
- The rules protecting that data are different:
  - United States
  - EU
  - The rest of the world….
- If dealing with PII or PHI, there may be a need to avoid having data crossing borders.

What kind of expertise is necessary?

- Evaluate your security procedures against your needs.
- Does my organization have the resources and know-how to comply on its own?
- Is compliance the highest and best use of my organization's resources?

What type of cloud service categories: are you considering?

Public Cloud

Customers access cloud services and store documents in large datacenters equipped with hundreds of virtualized servers that house data from multiple organizations.

Private Cloud

A single organization uses a dedicated cloud infrastructure.

Community Cloud

A private cloud is shared by a group of organizations with common missions, interests, or concerns. For example, a cloud provider may offer an instance of their services in a cloud dedicated for only government customers.

Hybrid Cloud

A private cloud is extended to the public cloud to extend an organization's datacenter; or two or more cloud types are linked to enable data and applications to flow between them in a controlled way.

What type of cloud infrastructure are you considering?

Cloud Service Categories:

- **Software as a Service (SaaS)**

The cloud provider hosts a single application, or a suite of programs which includes a mix of products.

- **Platform as a Service (PaaS)**

Users create and run their own software applications while relying on the cloud provider for software development tools as well as the underlying infrastructure and operating system.

- **Infrastructure as a Service (IaaS)**

Users rent computing power—either actual hardware or virtual machines—to deploy and run their own operating systems and software applications.

FOLEY HOAG LLP

What are the key substantive requirements of ISO 27018 for handling customer data?

Key Elements of ISO 27018

What does it cover?

What is the concerns?

What are the key elements of ISO 27018?

- All elements of PII/PHI are covered by ISO 27018
- All types of industries fall within the scope of ISO 27018
- ISO 27018 applies to any size company

Key Elements of ISO 27018 (cont.)

What does it cover?

What is the concerns?

What are the key elements of ISO 27018?

- Need for clarity and simplicity
- Extensive time and expense of complying with different standards
- Lack of uniformity across industries, jurisdictions
- Worldwide recognition of security standards
- Standards that hold up against audits, customer inquiries and government reviews

Key Elements of ISO 27018

What does it cover?

What is the concerns?

What are the key elements of ISO 27018?

- Specifies guidelines for the protection of PII.
  - These protections are based on ISO 27002, taking into consideration the regulatory requirements that might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.
- Commonly accepted control objectives, controls and guidelines.
  - This includes guidelines for implementing measures to protect public cloud computing in accordance with the privacy principles in ISO 29100.
- Under ISO 27018, compliant CSPs will not use customer data for their own independent purposes (such as advertising and marketing) without the customer's express consent, and not tie the agreement to use the services to the CSP's use of personal data for advertising and marketing.

Key Elements of ISO 27018

What does it cover?

What is the concerns?

What are the key elements of ISO 27018?

- Establishes clear and transparent parameters for the return, transfer and secure disposal of personal information.
- Requires CSPs to disclose the identities of any sub-processor they engage to help with data processing before customers enter into a contract.
  - And if any of the CSP changes subprocessors, the CSP is required to inform customers promptly to give them an opportunity to object or terminate their agreement.

FOLEY HOAG LLP

How does ISO 27018 adoption benefit customers in regulated industries such as healthcare and financial services?

Benefits of ISO 27018 Adoption

- The standard covers a wide range of subjects.
- It removes needs for negotiations over privacy and security standards.
- Demonstrated adherence to ISO 27018 allows a CSP to show that its cloud privacy policies and practices are consistent with the industry's best practices.
- Regulators like it, because they see it as assurance of compliance with their own country's data protection rules.

FOLEY HOAG LLP

How do the ISO 27018 requirements map against existing sector-based data privacy and security standards (e.g., HIPAA, SSAE/SOC 2)?

ISO 27018 is applicable to all types and sizes of organizations

This includes:

- public and private companies,
- government entities,
- not-for-profit organizations,

If they provide information processing services as PII processors via cloud computing under contract to other organizations.

ISO v. SSAE

- SSAE 16 (Statement on Standards for Attestation Engagements No. 16), the successor to SAS 70, and ISAE 3402 (International Standards for Attestation Engagement No. 3402), are audit standards established by the American Institute of Certified Public Accountants (AICPA) and the International Auditing and Assurance Standards Board of the International Federation of Accountants.
- SSAE 16 and ISAE 3402 are geared towards service organizations (entities that provide outsourcing services that impact the control environment of their customers, e.g., insurance and medical claims processors, hosted data centers, application service providers and managed security providers).

ISO v. SSAE (cont.)

- SSAE 16 and ISAE 3402 audits are independent verifications of compliance with security controls and effectiveness of security controls.
- At the conclusion of an SSAE 16/ISAE 3402 service auditor's examination, the service auditor renders an opinion on the following information:
  1. Whether or not the service organization's description of controls is presented fairly.
  2. Whether or not the service organization's controls are designed effectively.
  3. Whether or not the service organization's controls are placed in operation as of a specified date.
  4. Whether or not the service organization's controls are operating effectively over a specified period of time. (SSAE 16 (SOC 1) Type II and (SOC2) Type II only).

ISO v. SSAE (cont.)

- SSAE 16 has been predominantly used in the United States to provide a standard for audits of the design and effectiveness of controls.
- ISO 27001 is **an international standard** geared towards security practices of an organization.
- ISO 27001 is common in Europe, Japan and some other Asian countries, but **is gaining popularity in the United States**.

ISO v. SSAE (cont.)

- ISO 27001 stipulates a set of security controls and certifies against those controls; it is more comprehensive in coverage than SSAE 16.
- Organizations may be certified as compliant with ISO 27001 by a number of Accredited Registrars worldwide.

ISO v. HIPAA

ISO 27018 mirrors some of HIPAA while also providing a third-party review mechanism.

- ISO 27018 focuses on PII, but can serve as a guide for a technology service provider handling PHI.
- ISO 27018 and HIPAA overlap significantly.
- It bridges the gap HIPAA leaves for those entities that touch health information, but are not HIPAA covered entities or HIPAA business associates.
- Technology service providers that have successfully undergone a successful audit for the controls under ISO 27018 demonstrates a commitment to using security and privacy controls that is applicable under HIPAA.
- However, ISO 27018 does not eliminate the need for HIPAA business associate agreements.

See *Commentary: Healthcare must embrace new ISO cloud privacy standard*, April 27, 2015, Julie Anderson, SafeGov, http://www.govhealthit.com/news/commentary-healthcare-must-embrace-new-iso-cloud-privacy-standard

FOLEY HOAG LLP

What value is provided by third party verification (through accreditation) of ISO 27018 and other data privacy and security practices in cloud computing?

FOLEY HOAG LLP

The Value of ISO 27018

- **Compliance**: Look to work with CSPs that are verified as ISO 27018 compliant.
- **Accreditation**: In order to be so certified, a CSP must go through a rigorous process, under the auspices of an accredited and independent certification body.
- **Regular Reviews**: And to remain compliant, a CSP must subject itself to regular third-party reviews of its adherence to ISO 27018.

FOLEY HOAG LLP

Next Steps

- Review your company's existing CSP agreements, to see what they say about compliance with existing cloud standards, including ISO 27018.
- Cloud users should ask their current CSPs if they are now (or are planning to be) ISO 27018 compliant.
- Consider amendments to CSP agreements to add ISO 27018 compliance.

Thank you!

For follow-up, please contact:

Colin J. Zick, Esq.

Partner and Co-Chair, Privacy and Data Security Practice Group

Foley Hoag LLP

czick@foleyhoag.com

(617) 832-1275