How to Secure Private Data Stored and Accessed in the Cloud

Principle(s) Addressed
Address Privacy & Security, Understand the Ecosystem

Overview

By implementing appropriate safeguards, policies and procedures, private data can be securely stored and accessed in third-party cloud servers by a network of users.

Key Terms:

- **Administrative safeguards** refer to organizational policies, procedures and maintenance of security measures that are designed to protect private information, data and access. Examples include access groups, risk management plans, and workforce training and management.
- **Back-end security** relates to server-side processes and safeguards (in the case of third-party cloud services) enforced by the cloud service provider.
- **Cloud services** are facilities managed by third parties that store data (e.g., Google Drive and G Suite, Dropbox, email providers like Gmail and Outlook.com, Amazon S3, web hosting companies, etc.)
- **Data** encompass user information (e.g., patient data), programmatic information (e.g., for monitoring and evaluation), digital information (e.g., text documents, spreadsheets, presentations, graphics) and digital communication (e.g., email, instant messaging).
- **Encryption** is the translation of data into another code that requires a private digital key to translate it back into readable form.
- **Front-end security** refers to user-enforced processes or safeguards restricting access to applications and data that users interface with directly.
- **Physical safeguards** restrict access to terminals, mobile devices and tablets linked to cloud networks or used for data collection and management. Examples include workstation and device access controls.

"Remember that technical security measures are only as strong as the human users of the technology. Design security that is usable in the contexts where the technology is used."

CLAYTON SIMS
Dimagi

- **Technical safeguards** are hardware, software or procedural mechanisms for security. Examples include two-factor authentication and encryption.
- **Third-party-hosted cloud services** are provided for a fee by an external organization, such as Google, Microsoft Corporation or Amazon.com. Examples of cloud-storage applications include Dropbox, Microsoft OneDrive and Google Drive. Examples of cloud-based application services include Onai and CommCare.
- **Two-factor or multi-step authentication** requires a user to provide two or more pieces of authenticating evidence before receiving access: generally, something the user knows (e.g., a password) plus something the user has (e.g., an access code). Multifactor authentication may include a biometric, such as a fingerprint.

Description

Securing data, devices and tools is paramount for protecting user privacy and ensuring that organizational data is not compromised [http://digitalprinciples.org/address-privacy-security/]. In addition, national and international regulations for data security and privacy — particularly around health infrastructure and personally identifiable information — are an increasingly important consideration for many organizations; these regulations include the African Union Convention on Cyber Security and Personal Data Protection, the European Union General Data Protection Regulation and the Asia-Pacific Economic Cooperation Privacy Framework [http://digitalprinciples.org/understand-the-existing-ecosystem/].

Cloud computing services are provided by a hosting service that stores and processes end-user data while providing data management services over the internet. Cloud storage reduces the financial and human resources needed within organizations to back up data and maintain server access. A cloud service facilitates data management and applications across a network linked through mobile devices, computers and tablets.[1]

However, these networks can pose significant challenges for front-end security in the cloud computing environment.[2] Multiple levels of user-enforced security safeguards are needed to restrict access, verify user identity, preserve data integrity and protect the

"Our collective bias is on data minimization. But data are worth billions of dollars of market capitalization. Let's own that. It's naive to think groups will minimize. If that's the case, how do we manage, define, control, and use data, particularly if we're going to have a meaningful conversation with the private sector."

WILLIAM HOFFMAN
World Economic Forum

[1] Kuo AM. Opportunities and Challenges of Cloud Computing to Improve Health Care Services. *J Med Internet Res.* 2011 Sep 21;13(3):e67. doi: 10.2196/jmir.1867. Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3222190/.

[2] Yunchuan S, Zhang J, Xiong Y, Zhu G. Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks.* 2014 Jan 1;10(7). doi: 10.1155/2014/190903. Available at http://journals.sagepub.com/doi/full/10.1155/2014/190903#.

privacy of individual data. Moving to the cloud is an opportunity to standardize, replicate and deploy robust data-security processes across networks.

Organizations that store their data using a third-party cloud service benefit from the extensive security frameworks that reputable cloud service providers implement. Unlike typical user organizations, third-party cloud services employ thousands of security workers and enforce security safeguards that are sophisticated and well-resourced. To further protect the integrity and confidentiality of highly sensitive data in the cloud, users need to implement front-end technical, administrative and physical security safeguards.

This guide outlines steps to promote modern and robust front-end security when using third-party cloud services. Combined with the extensive security protocols implemented by cloud service providers, these practices yield an additional layer of protection for private data. These recommendations are summarized from existing references, which are noted in the Resources section.

Process

1. **Implement data confidentiality principles** that are appropriate to the level of sensitivity and confidentiality of data stored in the cloud. This step can be accomplished by enacting stronger principles for highly sensitive data to protect identity and confidential information. Administrative safeguards (e.g., risk evaluation and management, access restrictions), technical safeguards (e.g., data encryption, user authentication) and physical safeguards (e.g., securing devices in a locked room) can all be used to protect highly sensitive or private data. (See Figure 1.)

2. **Implement data integrity safeguards** to protect data from unauthorized deletion, modification, fabrication or dissemination. This step is crucial due to interoperability across devices and systems when using cloud services. Authenticate user identities, and provide users with appropriate levels of data access and permissions based on their roles, defaulting to the minimum amount of permissions. (See Figure 1.)

> "Consider that any information shared through unencrypted SMS may be intercepted by the telecom or other parties, such as government agencies, and any information shared via shortcode may be accessible by third party aggregators and marketing companies."
>
> PETER MICEK
> Access Now

FIGURE 1: TECHNICAL, ADMINISTRATIVE, AND PHYSICAL SAFEGUARDS FOR DATA CONFIDENTIALITY AND INTEGRITY

SAFEGUARD	WHAT IT IS?	CONSIDERATIONS	REQUIREMENTS
Two-step or multi-factor authentication	Something you know (e.g., a password) plus something you have (e.g., a mobile phone with an access code). Multifactor includes something you are (biometric).	Challenging to implement in the field; can be expensive depending on the solution.	Enforce strong passwords for the first layer of protection. Use a cloud-based single sign-on system (e.g., Okta, OneLogin or Microsoft Azure Active Directory) to handle authentication to cloud services.
Encryption	Translation of data into another code that requires a private digital key to translate the data back into readable form.	Major cloud service providers encrypt user data in transit to and upon storage on their servers. Client-side encryption, or when a user adds a second layer of encryption before data are stored in the cloud, is only possible for cloud applications where data are stored as files, not as records (e.g., a non-software-as-a-service-application such as Box or Amazon Web Services). Encryption tools: Syncany [https://www.syncany.org] and GNU Privacy Guard [https://gnupg.org/].	Create encryption keys for devices, data and email. Develop and enforce encryption-key management practices.
Access groups	Users are grouped by specific privileges depending on their roles (e.g., read-only access, read/write access).	Users may request access to data and data-management permissions that are not appropriate for their use cases. Access revocation (i.e., turning off access when people leave a program or should no longer have access) requires oversight and action. Forwarding of access rights by users, a significant problem with document systems like Dropbox, can result in unauthorized access if not managed properly.	Default to minimal permissions for the majority of users. Document use cases correlating to data access and management permissions for transparency and to promote support from users.
Physical safeguards	Restricting physical access to terminals, mobile devices and tablets linked to cloud networks and/or used for data collection and management.	Users may access cloud services and stored data via personal devices that may not be regularly subjected to front-end security principles and updates.	Use cloud-based mobile-device management systems to enforce encryption and security policies on user devices. Ensure that all devices linked to the network are encrypted and that permissions are set, even for private mobile devices and computers.

3. **Create and document organizational data security policies.** Information security requires effective administrative, technical and physical safeguards. These safeguards apply when operating within either a cloud computing environment or a traditional server-based environment. However, when using cloud services, resources that were previously used to conduct server maintenance and backup can be diverted to develop, document, support and monitor security-management processes.

4. **Conduct a network risk analysis and set up a risk management strategy.** Assign responsibility for security and risk management to specific individuals. Conduct security awareness and training sessions for data users, ensuring that staff understand how to follow contingency plans and procedures in case of security emergencies and incidents. Consider data localization requirements and which possible adversaries (e.g., government actors) could access via legal requirements for in-country operations, mutual legal assistance treaties or data requests, or through physical access to data storage or backdoored encryption [https://transparencyreport.google.com/user-data/overview].

5. **Monitor implementation and conduct compliance audits.** Carry out periodic audits to identify security vulnerabilities and monitor compliance. Create and implement policies for workforce management and discipline related to security breaches; decide how your organization will be accountable. Learning is achieved through doing, not telling; provide professional development appropriate to the level of data handled.

6. **Follow best practices for highly sensitive and private data** to further protect identities and confidential information of individuals whose data will be stored in the cloud. Refer to national guidelines for collection and storage of private data, specifically whether policies allow these data to be stored in the cloud. National and international regulations also provide guidance on best practices [http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm], [http://www.eugdpr.org/] and [https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection].

Outcomes

These outcomes are illustrative and have been collected from digital development organizations that have followed the steps outlined in this guide.

- Modern and robust security principles are deployed using the cloud service provider's security infrastructure.
- Resources for in-house server operations and maintenance are reallocated to upgrade and maintain robust security safeguards via cloud-based services.

PROCESS

TIPS AND RESOURCES

Privacy Recommendations for Information and Communication Technologies for Health and Development
(Adapted from Global Pulse http://www.unglobalpulse.org/sites/default/files/Data%20Privacy%20and%20Security%20in%20ICT4D%20-%20conference%20report%20layout%20-%20FINAL.pdf)

1. Build proactive privacy mechanisms into initiative design.
2. Be transparent with individuals whose information is collected about how the data will be used.
3. Maintain the purpose of personal data collected for specific, fair and justified use.
4. Minimize the amount and detail of data collected to only the essential.
5. Enforce principles for storage time and destruction of data.

- Best practices for collecting and protecting private data are followed, including determining if national and regional regulations allow for sensitive data (e.g., patient information) to be stored and accessed via the cloud.

Common Missteps

- **Data residency policies.** Policies and regulations in specific countries may discourage or prohibit the storage of data in offshore cloud services. The 2013 OECD Privacy Guidelines provide guidance for addressing issues of data ownership when data are transferred across borders [http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm]. National and international regulations may also restrict storage of patient or private data using cloud services.
- **Infrastructural limitations.** Limited or inconsistent internet bandwidth can make cloud services appear slow or unreliable to end users. Before implementing cloud services, organizations should assess network connectivity in the settings where users will need to access the services
- **Funding and resourcing.** Cloud services require access to stable ongoing funds to prevent services from being disconnected and data from being deleted. There are also costs for developing, implementing, maintaining and evaluating privacy and security measures. Organizations should assess whether they have access to stable, dedicated funding to support cloud services and security measures.
- **Rapidly changing technology and environment.** Users need a high level of technical expertise and awareness to adapt to changes in the cloud computing environment. Training users and attracting and retaining a technically sophisticated workforce have implications for funding.
- **Back-end security and privacy risks.** Cloud storage providers have some level of access to data (though highly restricted), which may cause a lack of confidence in data security and privacy for users. Security compromises are also possible as a result of cyberattacks or cloud service provider internal breaches.

> "There's often confusion between consent, understanding, and choice. They're not the same thing. People can be overwhelmed by information. Even where people understand, sometimes consent is not choice unless there are meaningful alternatives."
>
> — KATHY JOE
> ESOMAR

RESOURCES

FIELD IMPLEMENTATION GUIDANCE:

Conducting Mobile Surveys Responsibly: A Field Book for WFP Staff, World Food Programme (WFP). http://documents.wfp.org/stellent/groups/public/documents/manual_guide_proced/wfp292067.pdf

Girl Safeguarding Policy: Digital Privacy, Security, & Safety Principles & Guidelines, Girl Effect. http://www.girleffect.org/media/3052/gem-girl-safeguarding-policys_19-05-16.pdf

Responsible Data Management, Oxfam. http://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management

TECHNICAL GUIDES:

Audit Trail and Node Authentication, Integrating the Healthcare Enterprise (IHE). http://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication

Cloud Computing Toolkit, HIMSS. http://www.himss.org/library/healthcare-privacy-security/cloud-security/toolkit

Doing It Right: Cloud Encryption Key Management Best Practices, TechTarget Network. http://searchcloudsecurity.techtarget.com/tip/Doing-it-right-Cloud-encryption-key-management-best-practices

Enabling Privacy: Data Segmentation, HealthIT.gov. https://www.healthit.gov/providers-professionals/ds4p-initiative.

IT Infrastructure Handbook: De-identification, IHE. https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_De-Identification_Rev1.1_2014-06-06.pdf.

IT Infrastructure Technical Framework Supplement: Data Segmentation for Privacy, IHE. http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_DS4P_Rev1.0_PC_2014-03-14.pdf.

PRIMERS AND BACKGROUND:

Cloud Computing in Health White Paper, Canada Health Infoway. https://www.infoway-inforoute.ca/en/component/edocman/545-cloud-computing-in-health-white-paper-full/view-document?Itemid=0.

Cross-Enterprise User Assertion (XUA), IHE. http://wiki.ihe.net/index.php/Cross-Enterprise_User_Assertion_(XUA).

Data Protection, Privacy, and Security for Humanitarian & Development Programs, World Vision International. http://www.wvi.org/health/publication/data-protection-privacy-and-security-humanitarian-development-programs

"Unless we react quickly, there's going to be a data scandal. Someone's database with lots of sensitive information is going to get exposed. [Development organizations] have tons of this data, [. . .] consultants have it, [and it's stored on] laptops. This is very intimate, private information. We are adamant that our personal information is protected, but everybody has rights to these protections, not just us. So the question becomes how do we equip organizations with the policies, practices, and standards that enable these protections, particularly when moving from analog to digital tools."

MALIHA KHAN

Independent consultant

Improving Data Privacy & Security in ICT4D: A Workshop on Principle 8 of the Digital Development Principles, United Nations Global Pulse. http://www.unglobalpulse.org/sites/default/files/Data%20Privacy%20and%20Security%20in%20ICT4D%20-%20conference%20report%20layout%20-%20FINAL.pdf

A Primer on the Privacy, Security, and Confidentiality of Electronic Health Records, MEASURE Evaluation. https://www.measureevaluation.org/resources/publications/sr-15-128-en

Quality, Research and Public Health (QRPH) White Paper: Using IHE Profiles for Healthcare — Secondary Data Access, IHE. https://www.ihe.net/uploadedFiles/Documents/QRPH/IHE_QRPH_WP_Healthcare_Secondary_Data_Access.pdf

Responsible Data Policies – Terms, Policies and Frameworks. MERLTech. https://drive.google.com/file/d/0B6RRlwWznhZqalBVS3FlTEVZVmc/view

REGULATION AND POLICY:

African Union Convention on Cyber Security and Personal Data Protection. https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

European Union General Data Protection Regulation (EU GDPR). http://www.eugdpr.org/

Guidance on HIPAA & Cloud Computing, U.S. Department of Health and Human Services (HHS). https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

"There's still a view that technology will solve anything. But there's a growing understanding that technology also comes with real challenges and ethical quandaries."

ELLA DUNCAN

Search for Common Ground