Telehealth Risk Management

Early Release Edition

cloud security alliance®

The permanent and official location for the Health Information Management Working Group research is:
https://cloudsecurityalliance.org/research/working-groups/health-information-management/

Acknowledgments

Lead Authors

Dr. James Angle

CSA Global Staff

Diego Diviani
Michael Roza
Patty Ryan

Reviewers

Ashish Vashishtha

CSA Global Staff

Vince Campitelli
Alex Kaluza
AnnMarie Ulskey (Designer)

The CSA's Health Information Management Working Group aims to directly influence how health information service providers deliver secure cloud solutions (services, transport, applications, and storage) to their clients and foster cloud awareness within all aspects of healthcare and related industries. The working group research will continue to be freely available for use without license fees or restrictions by the CSA.

Table of Contents

1.0 Introduction

The COVID-19 pandemic has increased data demand and accelerated the practice of telehealth for medical professionals. The Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) defines telehealth as electronic information and telecommunications technologies to support and promote long-distance clinical healthcare, patient and professional health-related education, and public health and health administration. Technologies include videoconferencing, the internet, store-and-forward imaging, streaming media, and landline and wireless communications[1].

A Healthcare Delivery Organizations (HDO's) ability to manage telehealth data and associated processes are essential components of data security and data privacy. Developing and implementing a risk management program for telehealth requires a strong governance program. Robust HDO governance mechanisms underscore a commitment to reliable information and risk management practices in compliance with all applicable laws, standards, and regulations.

A good governance program will provide the following benefits:

- Help the HDO understand and prioritize stakeholder expectations.
- Allow the HDO to set business objectives that are congruent with values and risks.
- Keep the HDO in compliance with legal, contractual, internal, social, and ethical requirements.
- Improved quality of care for patients.
- Improved data quality resulting in improved public health.
- Increased operational efficiency and effectiveness.
- Better risk-based decisions and risk management (American Health Information Management Association, 2014).

Governance is an effective means for organizations to gather important risk data and manage risks while reporting results to management. This data enables management to set budgets and make risk-based decisions. Additionally, governance provides a view of an HDO's risk posture, allowing management to make risk-based decisions on allocating resources and mitigating risks effectively throughout the data lifecycle.

During the pandemic, telehealth governing rules changed dramatically—a shift that prompted HDOs to update and revise their governance and risk programs quickly. With the rapidly changing demands and evolving telehealth regulatory requirements, HDOs need effective governance and risk programs to ensure a smooth and seamless transition while improving their current risk postures (Angle, 2020).

[1] https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf

2.0 Governance

Governance is the foundation of any privacy and security compliance efforts. The term is defined as a management approach through which executives direct and control an organization (using a combination of management information and hierarchical management control structures). Information governance establishes the system, strategy, policies, procedures, guidelines, laws, and regulations that HDOs must adhere to.

Information Governance Framework				
	Strategy (Determines context and objectives)	Information Strategy		
Why do I need to do this?	Policies (Identifies issue & scope)	Information Rights Policy	Information Compliance Policy	Information Security Policy
What is required?	Standards (Assigns quantifiable measures)	e.g. Encryption/Password, Data Retention and disposal, Privacy Notices, Roles and Responsibility, Training etc.		
How do I do it?	Procedures (Establishes proper steps to take)	e.g. Subject Access Requests, CCTV/Surveillance, Data Incident Response, Data Protection assessments etc.		
	Guidelines (Establishes expected good practice)	e.g. use of personal removable media, clear desk guidelines etc.		

Figure 1: Information Governance Framework, adopted from Nottinghamshire County Council

Effective information governance extracts value from data and how it is managed throughout its lifecycle. Data lifecycle management is critical because data value may decline over time. However, data storage costs and exposure risks do not. When reviewing data lifecycles, it is helpful to use common cloud computing terminology (which divides the data lifecycle into the following concepts)[2]:

1. **Create:** Data is generated, acquired, or modified.
2. **Store:** Data is committed to a storage repository.
3. **Use:** Data is processed, viewed, or used in any other sort of activity.
4. **Share:** Data or information is made accessible to others.
5. **Archive:** Data is placed in long-term storage, per data retention guidelines and legal obligations.
6. **Destroy:** Data is no longer required and made inaccessible.

Data lifecycle should follow the privacy by design principles and privacy laws (e.g., New Zealand's HIPC 2020). Healthcare delivery organizations should embed these principles throughout the telehealth project lifecycle of every telehealth initiative and—at a minimum—conduct a privacy impact assessment (PIA) to analyze risks and required mitigations.

Create

Healthcare delivery organizations create and collect data for numerous reasons (e.g., financial, patient management) and in diverse environments (e.g., supply chains, human resources). The essential governance questions in this stage include:

1. What is the purpose of this health information collection? Have the affected individuals consented to this collection?
2. How is the data created, collected, or modified? Is the data produced by an external source (i.e., a new patient or employee entering the initial data)? Is it created by compiling data for other sources? Is it collected by keyboard entry, mobile application, or combining data? The HDO must know the origins of all data.
3. What will the data be used for? This is critically important for HDOs. Personally identifiable information (PII) and protected health information (PHI) laws require HDOs to inform the data subject what the collected information will be used for.
4. Who can create or collect data? Identifying who creates or collects data is particularly important when the information contains PHI and can alleviate data integrity concerns.
5. What is the data classification and categorization? Data classification relates to the confidentiality requirements for data types. For example, data may be designated as for "internal use only," "business-sensitive," or "PHI sensitive." "Categorization," as defined in the Federal Information Processing Standards (FIPS) 199, establishes three potential levels of impact ("low," "moderate," and "high") relevant to securing information and information systems for each of the three stated security objectives (CIA Triad: "confidentiality," "integrity," and "availability") (Stine et al., 2008). There are also military classifications ("top secret," "secret," "confidential," and "unclassified") and business classifications ("highly sensitive," "sensitive," "internal," and "public") that can be considered.

[2] Cloud Security Alliance, Security Guidance for critical Areas of Focus in Cloud Computing, Pages 62 and 63

6. How secure are each of the tools leveraged to create data? Has the vendor implemented secure development practices (including application code scanning and appropriate access control to code) and protected their intellectual property?

Understanding data sources enables organizations to build solid governance foundations.

Store

An HDO storage management policy should allow HDOs to effectively manage storage resources while complying with all laws and regulations. Before HDOs can determine storage requirements, they must understand how much and what type of data they are storing. The following questions can help start this conversation.

1. How do you ensure data quality, including the right to collect the information (or to be forgotten)?
2. How do you ensure data is not used for other purposes beyond informed consent?
3. Where will the data be stored? In the cloud, an enterprise data center, locally stored, or on removable storage media? Each of these scenarios has different requirements, and HDOs should consider the implications associated with each option.
4. Who has access to the data in storage? This is critical to understanding the access privileges of those responsible for managing the data storage infrastructure.
5. For data in the cloud, where is it stored? It is essential to know where data is stored, both primary and backup information. Is the data stored offshore? Regulatory requirements may differ depending on the storage locale.
6. How long will the information be required? Retention requirements may drive the storage method.
7. Is there a requirement for encrypting data at rest? Due to data sensitivity, there may be a regulatory or business requirement for encryption.

Knowing what type of data is being stored, where it is stored, who has access to it in storage, its state in storage, and how long it is required will enable HDOs to create data storage policies and procedures.

Use

As data collection increases in speed and scale, the analytic techniques used to process these datasets become more sophisticated, and data use becomes more varied. Big data analytics will continue to expand the use of telehealth data. There is enormous potential for big data in health research; however, proper care must be taken to prevent data loss or misuse. Additionally, transparency presents a complex challenge for healthcare data governance. Effective data governance enables positive outcomes and stops negative consequences. Healthcare delivery organizations must be transparent about data use while maintaining privacy and security.

Understanding the data and how to use it is the first step. Additionally, healthcare delivery organizations must know the answers to the following inquiries:

1. Who is the data user? The data user may not be the data owner (i.e., a nurse or doctor reading a patient's electronic PHI (ePHI) during an appointment).
2. Where will the data be used? (i.e., analyzing geo-location jurisdictions)
3. How do you ensure data is not used for other purposes beyond informed consent?
4. What is the purpose of the data, and how will it be used?
5. Is that use appropriate based on data type and regulatory requirements?
6. How will the data be used in the future?

The first step HDOs must take is to classify and categorize the data to help answer these questions. Gaining a complete understanding of the data and users will help implement controls that efficiently and effectively protect the data. Additionally, HDOs must know how data will be used.

Share

For years, HDOs built data repositories that were silos where data was confined and isolated. The use of these silo systems led to building systems where data was duplicated rather than shared. Good data governance can provide the processes required to share data effectively. Data transmission policies include appropriate data transmissions, encryption requirements, and acceptable transmission mechanisms. To that end, HDOs must answer the following questions:

1. With whom will the data be shared? (i.e., an insurance company, billing resources, hospital/treatment staff)?
2. For what purpose will the information be shared? Are these reasons valid?
3. Is that use appropriate based on data type and regulatory requirements?
4. Will the information ever leave the telehealth infrastructure (e.g., via interfaces or file transmission/email to other service providers)? Can the data be adequately protected when used/stored by these additional providers?

Archive/Destruction

Laws and regulations—such as the Health Insurance Portability and Accountability Act (HIPAA)—demonstrate the need for effective plans for managing the endless array of data that HDOs are creating, processing, and storing. Healthcare delivery organizations must implement information governance policies to minimize liabilities, improve operations, and reduce costs. Data that is no longer in active use can and should be either destroyed or archived. It is critical that HDOs fully understand whether data requires long-term storage (which can bear considerable financial and technical burdens). Archiving data can reduce storage expenses, and long-term storage is cheaper than short term. But HDOs must not forget that data destruction, including asset disposal, is the critical last phase of any data lifecycle. As sensitive, regulated data is leveraged and stored across many locations, HDOs must implement clear, concise policies and procedures to destroy outdated and restricted data (and the media on which it is stored if unencrypted). This process involves two crucial considerations: data retention policies and data disposal policies.

Accordingly, HDOs must answer the following questions:

1. What are the data retention requirements for the various data types within an HDO's control globally?
2. Does each partner who stores ePHI as part of the telehealth service have the means to meet any data archiving requirements?
3. Who is responsible (considering segregation of duties) for data destruction?
4. What assurance do the partners provide that data is securely destroyed per agreed-upon retention guidelines?
5. What are the destruction controls to ensure information is rendered unreadable?
6. Are data in an active litigation hold maintained until the conclusion of the hold? (Crosbie, 2020)
7. Who is responsible for asset disposal?
8. When an asset is no longer required, is the data on the asset adequately destroyed?
9. Has the physical storage capability been removed and the data destroyed?
10. Does the data destruction policy identify the procedure to ensure all sensitive data is destroyed?
11. When an asset is no longer required, is the information on the asset adequately destroyed or otherwise rendered inaccessible?
12. Has the physical storage capability been removed (and the data destroyed) or otherwise rendered inaccessible?

Data destruction for a single entity in a multi-tenant cloud environment is difficult, as the media cannot be destroyed for just one entity; it is an all-or-nothing situation. The most effective way to ensure data destruction is to encrypt the data at rest so the keys are destroyed when the data is no longer required. While the data is still physically there, it can never be used (Gillian 2019). One note about this method is that the HDO must ensure that each tenant has different encryption keys. This can be accomplished through implementation of a Key Management System that does not allow keys to be issued twice as well as tracking the issuance, use, destruction and recovery of each key.

3.0 Privacy

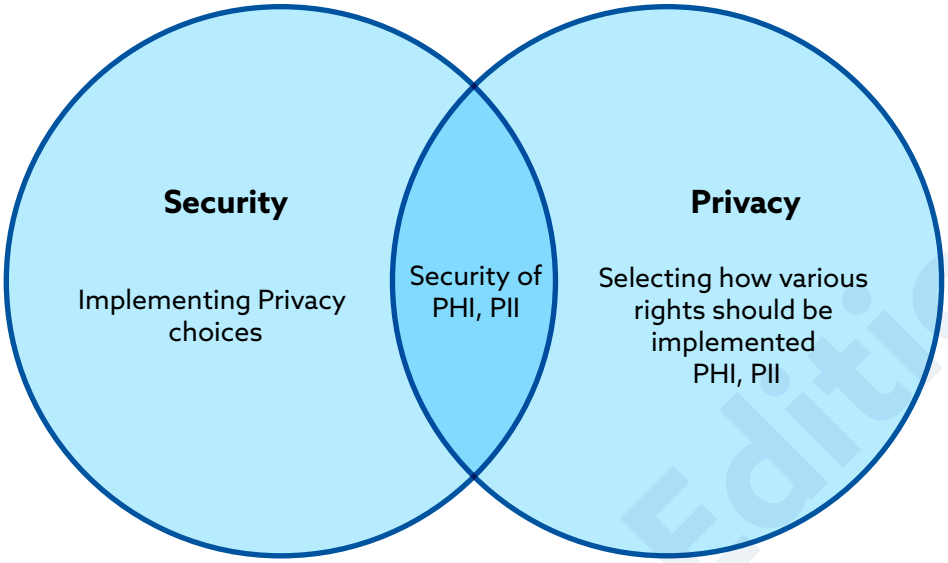

Figure 2: Cybersecurity and Privacy Risk Relationship

While there are numerous articles on "cloud security" and "cloud security and privacy," there are relatively few on "cloud privacy" as a standalone topic. Separating "privacy" from "security" brings a different meaning to how we view privacy and protect privacy. Security and privacy can, and should, be treated as distinct concerns. Privacy discourse involves decisions about legitimate, competing claims related to information access, use, and alteration (Bambauer, 2013).

Privacy is about selecting how various rights should be implemented; security is about implementing those choices. Separating privacy from security has significant practical consequences. Privacy establishes a framework for deciding who should legitimately have the capability to access and alter information. In healthcare, the invasion of patient privacy is a growing concern due to the emergence of advanced persistent threats and targeted attacks against information systems. Driven by COVID-19 and rule changes by the Office of Civil Rights (OCR), there has been a significant increase in the adoption of telehealth and an increased use of big data (Department of Health and Human Services, 2020). This expansion necessitates an increased awareness of privacy issues.

Technology has driven unprecedented innovation, economic value, and improvement in social services. In healthcare, the cost associated with the technology is connected to the collection of PHI. Ideally, technology optimizes individual benefits while protecting privacy. However, the tremendous volume of PHI stored in the cloud only elevates privacy concerns.

Healthcare delivery organizations must understand the relationship between privacy and security—and particularly the differences. This awareness will enable HDOs to implement privacy risk management programs to address privacy concerns. Additionally, HDOs must address PHI and PII concerns and provide mitigating controls for both information types.

Privacy Regulation

Most countries have data protection laws that govern health data processing. These regulations may be established in national law (which generally apply to personal data), sectoral laws (which apply to certain fields, such as healthcare), or specific laws (which apply to targeted scenarios, such as COVID-19). Each rule features unique requirements which may supplement another law or be an exception to another law. Most countries prohibit personal data transmission (including health data) to outside countries unless certain conditions are met. This paper only mentions two requirements: HIPAA and the General Data Protection Regulation (GDPR). While HIPAA and GDPR provide a relevant framework for this discussion, they are not the only pertinent laws related to personal data. Therefore, it is vital to understand regulations governing data collection, processing, and storage at the local and national levels.

HIPAA

The fundamental goal of HIPAA is to protect and disseminate PHI to enable high-quality healthcare. While HIPAA allows HDOs to share some data (e.g., treatment, payment, or health care operations data), they must obtain a patient's written authorization to allow data disclosures not explicitly authorized. All authorizations must be in plain language and contain specific information regarding the data disclosure, such as who will receive the information, data expiration dates, and the right to revoke the disclosure.

Privacy matters must include three essential roles: the recipient, controller, and processor.

- **Recipient:** A natural/legal person, public authority, agency, or other body to which personal data are disclosed (whether a third party or not).
- **Controller:** A natural/legal person, public authority, agency, or other body which—alone or jointly with others—determines the purposes and means of processing personal data.
- **Processor:** A natural/legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

The U.S. Department of Health and Human Services established the following definition:

"The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections" (Department of Health and Human Services, 2013)

Advances in healthcare information distribution have driven unprecedented innovation, economic value, and service improvements. While healthcare data value is often connected to personal information collection, patients may not understand the full implications of this process. Ultimately,

health information should enhance care while protecting individual privacy, and privacy safeguards must allow for personal choices while providing effective risk mitigation (NIST, 2020).

GDPR

The European Union's GDPR may also apply in certain scenarios, depending on the data collected and data collection/storage locales. The GDPR's overarching goal is to protect the personal data of EU "data subjects" while enhancing individual rights on how data is used. Businesses that collect, process, or store EU data subject information must comply with the GDPR regardless of the business' location. Additionally, any data stored or processed in the EU is subject to the GDPR.

Furthermore, the GDPR contains restrictions for personal data transfers to countries outside the EU (third countries). Two conditions are defined:

- The destination is a third country that ensures adequate levels of data protection (a set of criteria specified under GDPR, Art. 45).
- The transfer may only occur with appropriate safeguards defined in GDPR, Art. 46.

There are several exceptions to the restrictions (e.g., a data subject's explicit consent for the proposed transfer or the transfer is necessary to protect a data subject's interests). Additionally, specific binding corporate rules may allow large international organizations to transfer personal data within the corporate group, as defined in GDPR, Art. 47/49.

For most international transfers, standard contractual clauses (SCC) provide valid, practicable contractual solutions. The SCCs feature approved templates for use between the EU controller and the non-EU controller/processor enforcing GDPR requirements.

Note: *One of the most important international privacy cases in recent history arose from a complaint against Facebook brought to the Irish Data Protection Commissioner by an Austrian privacy advocate named Max Schrems. In the complaint ("Schrems I"), Mr. Schrems challenged the transfer of his data (and the data of EU citizens generally) to the United States by Facebook, which is incorporated in Ireland. On Oct. 6, 2015, the Court of Justice of the European Union invalidated the Safe Harbor arrangement, which governed data transfers between the EU and the U.S. Instead, the Safe Harbor act was replaced by the EU-U.S. Privacy Shield. On July 16, 2020, the Court of Justice of the European Union issued a judgment declaring the European Commission's decision ((EU) 2016/1250) "invalid" as of July 12, 2016. The court determined the protection provided by the Privacy Shield provided adequate safeguards. As a result, the EU-U.S. Privacy Shield framework no longer provides a valid mechanism to comply with EU data protection requirements regarding personal data transfer between from the EU to the U.S. There currently is no agreement enacted.*

Adherence to existing regulations (such as GDPR and HIPAA) requires a thorough examination of data throughout its lifecycle.

Create

The term "create" is defined as the generation or acquisition of new data or the modification of existing data. Privacy considerations in healthcare settings relate to the creation of PHI/PII, including any information used to identify specific individuals or groups. Privacy regulations increasingly mandate that individuals have the following rights in the creation stage:

- Understand what data will be collected and used for, and if it will be shared.
- Receive all explanations and justifications of HDO data collection practices in clear, simple language.
- Explicitly agree to data collection, processing, usage, and sharing.

At this early stage, it makes the most sense for HDOs to complete three other items:

- Specifically define who can collect PHI/PII.
- Create an organizational data map outlining access rights.
- Classify data based on sensitivity and value.

Store

In the privacy context, "data storage" means the housing and management of personal information (either in physical or electronic format). Healthcare delivery organizations are responsible for:

- Ensuring data privacy wherever data is stored, including appropriate controls based on data classification.
- Developing and implementing means for individual access to personal information, including individuals' abilities to correct errors and request personal data removal.
- Developing clear documentation pathways to explain:
  - How is data stored?
  - What are the data storage strategies?
  - How is data cross-referenced?
  - How long is information retained?

Use

Privacy regulations give individuals certain rights when their data is used. Some of these rights include:

- Individuals are entitled to know precisely how data is collected and used.
- Individuals can ask what information has been collected about them.
- Individuals can request to correct erroneous data.
- Individuals can request data deletion from records; however, medical professionals do not have to approve the request.
- Individuals can refuse to participate in data processing (i.e., marketing efforts).

All HDOs must have a privacy policy and privacy notice that explains what they do with user information.

Privacy policies must:

- Include contact details of the company and its representatives.
- Describe why the company is collecting the data.
- Define how long the information will be kept on file.
- Explain the user rights.
- Be written in simple language.
- Name the personal data recipients (if the company shares data with another organization).

Share

Shared data is information accessible to other parties, both internally and externally. The National Institute of Standards and Technology (NIST) refers to the data processing ecosystem to describe how data may be shared between different organizations. Healthcare delivery organizations should ensure that data loss prevention systems are used to detect unauthorized sharing or copying of sensitive data. Data processing ecosystems encompass various entities and roles that may have complex, multi-directional relationships with each other. An entity's role in the data processing ecosystem—which can affect its legal obligations—plays a crucial factor in privacy risk management strategies. A formal agreement/contract between HDOs and cloud service providers (CSPs) is required in the healthcare ecosystem.

Figure 3: Data Processing Ecosystem Relationships (NIST Privacy/ Framework, 2020

An effective data processing ecosystem addresses risk management concerns by clearly defining an organization's priorities, constraints, risk tolerance, and assumptions. These parameters support decision-making internally and with third parties within the data processing ecosystem. Furthermore, organizations should establish and implement processes to identify, assess, and manage privacy risks within the data processing ecosystem. It is critical to understand who has data access, under what circumstances data is accessible, and how PHI/PII is shared.

Archive

In general, except for PHI, all personal information should be deleted when no longer in use. Personal data must only be stored for the purpose it was collected and cannot be housed indefinitely. If underlying information may be required in the future, personal information can be disassociated from data before archiving. Disassociation enables data/event processing without association with individuals or devices beyond operational requirements (NIST, 2020). There are legal requirements to keep PHI for a set period.

Destroy

Unnecessary data should be securely discarded. Protected data should be removed from removable storage media containing private data before storage media disposal. All hard copies of such data must be finely shredded (preferably with a cross-cut shredder) before destruction. Destroy data in the cloud by encrypting data and destroying the keys or by data anonymization. Document when PHI/PII is destroyed, how it is destroyed, and who is accountable for its destruction.

Additionally, implement several measures to ensure data remains protected:

- **Clear desk policy:** Before any employee leaves, ensure that materials containing private data are not left on the employee's desk, and computers should be locked.
- **Password security:** No passwords are written down. Passwords should be long and complex.
- Practice secure storage: Store any material containing a person's private information securely. Digital data must be encrypted.
- **Mobile device security:** Devices should be adequately secured and be password-protected.
- **Ensure secure transmission of data:** Private information should not be sent via insecure means.
- **Secure data disposal:** Removable media that contains private data should not be disposed of without first ensuring that all protected data has been securely removed.
- **Reporting breaches:** Typically, organizations have 72 hours to report breaches.
- All employees must be trained to ensure they understand and adhere to all applicable privacy rules, policies, and procedures to minimize risks.

4.0 Security

While privacy considerations frame who can access, use, and alter information, security actions put this framework into motion. Security, therefore, is the interface between information and privacy. Security facilitates privacy rights, putting them into effect (Bambauer, 2013). Additionally, security provides protection for all HDO assets and identities while determining and protecting privileges (Haber et al., 2020).

Telehealth may become the new norm for the healthcare sector. Driven by the COVID-19 pandemic, telehealth is undergoing a dramatic, fundamental evolution in clinical operating, and business environments. Consumer demand for innovative, personalized, and convenient healthcare is fueling this demand (Abouelmehdi et al., 2018).

In the telehealth process, HDOs store, process, and transmit patient information. Data is a critical asset that requires HDOs to implement data security solutions that comply with healthcare mandates. Telehealth data may contain information requiring protection based on multiple, applicable regulations. For example, healthcare delivery organizations must comply with all rules for PII, as well as those established under HIPAA.

Each phase of the data lifecycle has unique requirements and should be viewed independently. While security requirements may overlap, phases should be assessed against phase requirements.

Create

The first step in the data lifecycle is creation. Any created data should fulfill a clear business need. Second, HDOs must have consent to collect PHI or PII. Data creation regulatory requirements depend on where data is created. For example, the GDPR requires security be built in at the time of data creation. Likewise, HIPAA requires protection for all PHI from inception to destruction. The bottom line: data must be created in a secure environment.

Store

Cloud data storage is complicated. Data owners must determine where data originated and where it is stored. Service providers must protect cloud data (including access control and encryption). Access control should be implemented within the management plane, application level, and internet sharing controls. Encryption or tokenization can protect data.

Additionally, the CSP should have a secure architecture that utilizes standard security best practices. These practices include robust monitoring, auditing, and alerting capability. A data loss prevention system can help identify who is using the data and their location. A CSP should complete a third-party assessment and offer to share that insight with the HDO.

Use

Geography determines the regulatory requirements for both stored and processed data. This can be a challenging concept, as telehealth solutions allow patients to access data from anywhere with internet access. For example, a patient can travel to the EU from the U.S. and videoconference back to their provider. In this case, the HDO is subject to the GDPR. Organizations should use federation and multifactor authentication whenever possible to access data. Identity and Access Management (IAM)—the process to manage individual access to digital resources—is a vital part of securing data in use. This process also determines what authorization individuals have regarding the data. Additionally, organizations should consider using an Application Programming Interface (API), which requires digital signatures to ensure security.

Share

Remember: not all data should be shared. However, when data sharing is required, the organization responsible for the data must ensure its security. As with data use, IAM is critical for data security. At a minimum, enact a Data Loss Prevention (DLP) program to discover, monitor, and protect data with regulatory or compliance implications in transit and at rest across the network, storage, and endpoints.

Sharing requires data transmission from the cloud to all applicable data users. Encrypt data while in transit and use a secure protocol. Use Transport Layer Security (TLS) 1.2 or higher.

Archive

Essential data that does not require frequent access or modification often resides in a data archive. Archiving data provides many benefits, especially in terms of efficiency. Encrypt archived data and control access to the information. Keep personal data or healthcare data only if required for its original, intended purpose.

Destroy

Since cloud data exists in a shared, dispersed environment, typical data deletion and destruction methods (such as wiping) cannot ensure all data copies are destroyed. Encryption, followed by key destruction, is the best guarantee to ensure responsible data removal.

Conclusion

Healthcare delivery organizations must have processes and controls enacted to ensure the privacy and security of telehealth patient information in the cloud concerning HIPAA and the GDPR (in addition to other potential regulations). Maintaining the sanctity and integrity of healthcare data is critical for regulatory reasons and patient safety. In this paper, the CSA's Health Information Management Working Group presented privacy and security issues in each phase of the data lifecycle and discussed methods to mitigate privacy and security concerns.

References

Abouelmehdi K., Beni-Hessane, A. & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of Big Data, Vol. 5.

American Health Information Management Association. (2014). Information Governance Principles for Healthcare. Retrieved from http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx

Angle, J. (2020). Information Technology Governance, Risk and Compliance in Healthcare. Retrieved from https://www.researchgate.net/search.Search.html?type=publication&query=Information%20Technology%20Governance,%20Risk%20and%20Compliance%20in%20Healthcare

Bambauer, D. (2013). Privacy Versus Security. The Journal of Criminal Law & Criminology. Vol. 103, No. 3.

Cloud Security Alliance. (2017). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. 62-63. Retrieved from https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf

Crosbie, D. (2020). Why Data Destruction is Essential to Information Governance. Complete Discovery Source. Retrieved from https://cdslegal.com/insights/why-data-destruction-is-essential-to-information-governance/

DataArchiva. (2018). The rising importance of data governance and archiving in healthcare. Retrieved from https://www.dataarchiva.com/the-rising-importance-of-data-governance-and-archiving-in-healthcare/

Department of Health and Human Services. (2020). OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency. Retrieved from https://www.hhs.gov/about/news/2020/03/17/ocr-announces-notificationof-enforcement-discretion-for-telehealth-remote-communications-during-the-covid-19.html

Department of Health and Human Services. (2013). Summary of the HIPAA Privacy Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Gillin, P. (2019) Data Destruction in the Cloud: It's Complicated. Retrieved from https://www.infogoto.com/data-destruction-in-the-cloud-its-complicated/

Haber, M., Rolls, D. (2020). Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution. Apress, doi 10.1007/978-1-4842-5165-2

National Institute of Standards and Technology. (2020). NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management. National Institute of Standards and Technology. Gaithersburg, MD. Retrieved from https://www.nist.gov/privacy-framework/privacy-framework

Stine, K., Kissel, R., Barker, W., Fahlsing, J., & Gulick, J. (2008). Special Publication 800-60 Volume I Revision 1: Guide for Mapping Types of Information and Information System to Security Categories. National Institute of Standards and Technology. Gaithersburg, MD. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final

U.S. Department of Health and Human Services. (2017). Guidance on HIPAA & Cloud Computing. Retrieved from https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html