Telehealth Data in the Cloud

cloud security alliance®

The Cloud Security Alliance (CSA) promotes the use of best practices for providing security assurance within Cloud Computing, and provides education on the uses of Cloud Computing to help secure all other forms of computing.

Acknowledgments

Lead Authors:

Dr. James Angle

Key Contributors:

Vincent Campitelli
Diego Diviani
Patty Ryan

CSA Global Staff:

Alex Kaluza
AnnMarie Ulskey (Design)

Table of Contents

Abstract

In the wake of COVID-19, health delivery organizations (HDOs) are rapidly increasing their utilization of telehealth capabilities—such as remote patient monitoring (RPM) and telemedicine—to treat patients in their homes. These technology solutions allow for the delivery of patient treatment, comply with COVID-19 mitigation best practices, and reduce the risk of exposure for health care providers. As COVID-19 progresses, telehealth solutions—which introduce high levels of patient data over the internet and in the cloud—could be used to remotely monitor and treat patients who have mild cases of the virus.

These trends will likely expand and evolve during the pandemic, as well as in a post-COVID environment. As the use of these capabilities increases, so do the security risks. As a result, infrastructure that supports telehealth deployment must diligently adhere to protocols regarding confidentiality, integrity, and patient data availability.

For example, third-party vendors using videoconferencing capabilities utilize cloud technologies with RPM devices to remotely monitor and manage patient care. This scenario presents a series of logistical challenges.

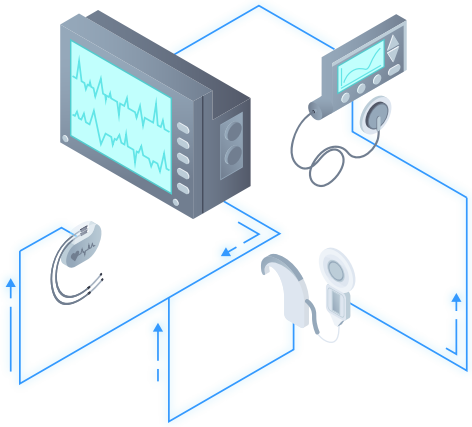
This paper will address the privacy and security concerns related to processing, storing, and transmitting patient data in the cloud, and expand this concept to include edge computing for telehealth solutions.

Introduction

The term "telehealth" is used interchangeably with "telemedicine." However, telemedicine is associated with the delivery of traditional clinical diagnosis and monitoring by technology and is a subset of the services encompassed by the term telehealth. Telehealth has a much broader definition that encompasses clinical health care as well as a wide range of other services. Telehealth uses innovative technologies, such as kiosks, website monitoring applications, mobile phone applications, wearable devices, and videoconferencing, to remotely connect health care providers to patients (Marcoux & Vogenberg, 2016).

Telehealth is becoming prevalent in the United States. As economic and resource constraints continue to impact the current method of health care delivery, the system is beginning to transition toward a patient-centric model. Most hospital systems utilize some form of telehealth for RPM. Additionally, with the onset of the COVID-19 virus, HDOs commonly rely on videoconferencing for routine outpatient visits. In-person visits to health care facilities are not required for routine appointments (except in certain cases, such as with laboratory or imaging visits). With the emergence of this highly infectious disease, this technology is urgently needed. Telehealth can dramatically bolster efforts to reduce patient exposure to other patients, staff members, and vulnerable populations if utilized effectively. It can also deliver needed care to individuals with mild symptoms in their homes while slowing the spread of a deadly virus.

The current guidance from the Centers for Medicare and Medicaid Services (CMS) broadens access to Medicare telehealth services—ensuring patients can receive a wider range of medical services without having to travel to a health care facility. Telehealth is ideal for providing health care to people who cannot easily access in-person services. Extolling the virtues of telehealth is part of a broader effort by CMS and the White House Coronavirus Task Force to ensure all Americans are aware of easy-to-use, accessible benefits that promote health and contain viral spread (CMS, 2020).



To deliver telehealth, platform providers commonly use videoconferencing capabilities and leverage cloud and internet technologies (in addition to RPM mechanisms). This environment provides an array of privacy and security challenges. For these reasons, it is vital to review the end-to-end architecture of a telehealth delivery system. A full analysis can help determine whether privacy and security vulnerabilities exist, what security controls are required for proper cybersecurity of the telehealth ecosystem, and if patient privacy protections are adequate.

Privacy Concerns

In the telehealth environment, privacy concerns abound regarding authorized information access, data usage, and data alteration. Privacy measures should establish a framework for deciding who should legitimately have the capacity to access and alter information (Bamauer, 2013). At the heart of privacy concerns related to telehealth is protected health information (PHI). The emergence of advanced, persistent threats and targeted attacks against information systems to access PHI is a growing concern. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule also provides insight for understanding telehealth›s privacy implications and is essential for shaping any discussions related to the issue.

> "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, 2003)

The HIPAA Privacy Rule regulates the collection use and disclosure of PHI held by HDOs and business associates. The Privacy Rule requires the HDO to notify individuals about how their PHI is used. The HDO must track all disclosures of PHI. Additionally, the HDO must have documented privacy policies and procedures. With exceptions for treatment facilitation, payment, or health care operations, the HDO must have written authorization to disclose PHI. The HDO must also minimize the information

it shares or communicates. Covered entities, business associates, and subcontractors used by business associates must protect PHI and comply with the HIPAA Privacy Rule.

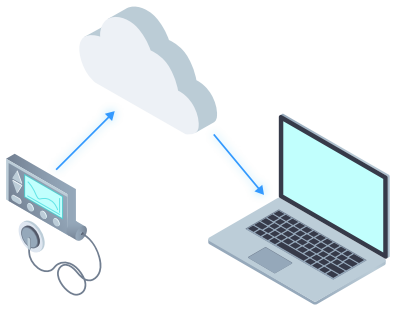
European Union (EU) General Data Protection Regulations (GDPR) may apply to PHI, dependent on where data is collected and stored. The main aim of the GDPR is to ensure the personal data of EU «data subjects» is protected and to increase the rights of EU data subjects over their data. Businesses that collect, process, or store the information of EU data subjects must comply with GDPR, regardless of a business location. If a cloud provider stores, processes, or transmits data in the EU, they are subject to the GDPR—which includes health information.

The GDPR gives individuals certain rights when their data is used, including:

- The right to know exactly how your data is collected and used
- The right to ask what information has been collected about you
- The right to correct data errors
- The right to delete data from records
- The right to refuse data processing (e.g., marketing efforts)

All businesses must have a privacy policy that explains what they do with user information.

These regulations can present daunting challenges for HDOs regarding data management—mostly dependent on where and how the data is stored. If information is offshore and commingled with other HDOs, it may be arduous to ensure complete data deletion.



HDOs need to know how cloud providers handle retention, audit, and monitor data access and usage. Additionally, in the event of a PHI breach, cloud providers should be able to show HDOs how they will notify the HDO and implement the appropriate privacy incident response with HIPAA breach notification. The provider should also be willing to sign a business associate agreement (BAA), a requirement under HIPAA. The BAA is a legal document between a health care provider and a contractor. A provider enters a BAA with a contractor or other vendor when PHI may be accessible to the contractor or vendor. Under a BAA, business associates must agree to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI.

The proliferation of PHI and the transition from structured to unstructured data has significantly increased the complexities and challenges of protecting individual privacy. In addition to this information security view, which focuses on confidentiality, there are implications for ensuring the integrity and availability of PHI (NIST SP 800-53 r4, 2013). To that end, the HDO should answer the following questions when entering into a telehealth agreement with a cloud provider:

1. Does the telehealth provider (TP) describe the purpose(s) for which PHI is collected, used, maintained, and shared in its privacy notices?
2. Does the TP have, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PHI?

3. Has the TP conducted a privacy impact assessment, and are they willing to share it?
4. Does the HDO have privacy roles, responsibilities, and access requirements for contractors and service providers?
5. Does the TP monitor and audit privacy controls and internal privacy policies to ensure effective implementation?
6. Does the TP design information systems to support privacy by automating privacy controls?
7. Does the TP maintain an accurate accounting of disclosures of information held in each system of records under its control, including:
    a. Date, nature, and purpose of each disclosure of a record; and
    b. Name and address of the person or organization to which the disclosure was made.
    c. The identity of who authorized the disclosure.
8. Does the TP document processes to ensure the integrity of PHI through existing security controls?
9. Does the TP identify the minimum PHI elements relevant and necessary to accomplish the legally authorized purpose of collection?
10. Does the TP provide means for individuals to authorize the collection, use, maintenance, and sharing of PHI before its collection?
11. Does the TP have a process for receiving and responding to complaints, concerns, or questions from individuals about organizational privacy practices?
12. Does the TP provide sufficient notice to the public and to individuals regarding its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PHI?
13. Does the TP share PHI externally?

Asking the provider these questions ensures the provider has a structured set of privacy controls that help comply with all applicable laws. Additionally, when viewed with the security controls, it demonstrates the relationship between privacy and security.

Security Concerns

Unlike internal networks, public cloud services are accessed over the public internet, and this must be considered when assessing security. While this is not an indication that the cloud is inherently insecure, security model development must take this reality into account. Stakeholders must consider end-to-end security, including internal policies for access control and user provisioning.

The HIPAA Security Rule requires the HDO to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI. Specifically, the HDO must ensure the confidentiality, integrity, and availability of all PHI created, stored, processed, or transmitted—and identify and protect against reasonably anticipated threats to the security and integrity of PHI. Additionally, HDOs must protect against reasonably anticipated impermissible use or disclosure of PHI. The Security Rule›s confidentiality requirements support the Privacy Rule›s prohibitions against improper uses and disclosures of PHI. The Security Rule also promotes the additional goals of maintaining the integrity and availability of PHI (HHS, 2003).

To ensure security, HIPAA requires HDOs to conduct a security threat-risk analysis. This assessment includes threats to cloud computing. Risk analysis provides information essential to making risk-

based decisions as they relate to telehealth. In addition to the risk assessment, the HDO should identify all the controls in place and ensure they are working as intended. It should be noted that security is a shared responsibility, and, in most cases, the HDO can only assess the controls within their own organization. The HDO will have to rely on a third-party assessment of the service provider's security controls. The third-party attestation can include a Service Organization Control 2 (SOC 2) report or HITRUST certification. Additionally, the service provider may be certified by FEDRAMP or the Cloud Security Alliance Security Trust and Assurance Registry (CSA STAR), which is a registry of certified cloud providers that have met security requirements.

As part of the assessment, the HDO should seek answers from cloud service providers to questions related to the following areas of concern: governance, compliance, confidentiality, integrity, availability, and incident response and management.

Governance

Governance includes the policies, procedures, and internal controls that comprise how the organization is run (CSA, 2917). Cloud computing transfers the responsibilities from the organization to a shared responsibility model.

1. Does the service provider's service-level agreement (SLA) clearly define how the service provider protects the confidentiality, integrity, and availability of all customer information?
2. Does the service provider's SLA specify that the HDO will retain ownership of its data?
3. Will the service provider use the data for any purpose other than service delivery?
4. Is the service provider's service dependent on any third-party stakeholders?

Compliance

Telehealth often delivers services that must comply with multiple regulations in multiple jurisdictions. The primary law in the U.S. is HIPAA, and in the EU, it is the GDPR.

1. Does the cloud service provider allow the HDO to directly audit the implementation and management of the security measures in place to protect the service and the data it holds?
2. Will the service provider allow the HDO to review recent audit reports thoroughly?
3. Is the service provider HIPAA compliant?
4. Does the service provider comply with the GDPR?

Confidentiality

As stated, confidentiality means protecting data from improper disclosure. The Health Insurance Portability and Accountability Act regulates the use and disclosure of PHI held by HDOs and business associates. The act requires that all individuals with access to PHI—including contractors and service providers—are "cleared" and have appropriate access to include following the rules for least privilege.

To ensure the accomplishment of these objectives, the HDO should address the following queries:

1. Authentication and Access Control
   a. Does the HDO have an identity management strategy that supports the adoption of cloud services?
   b. Is there an effective internal process that ensures that identities are managed and protected throughout their lifecycles?
   c. Is there an effective audit process to ensure that user accounts are appropriately managed and protected? Does the service provider meet those control requirements?
   d. Are all passwords encrypted, especially system/service administrators?
   e. Is multi-factor authentication required, and, if so, is it available?
   f. Does authentication and access control extend to devices?
2. Multi-Tenancy
   g. Will the service provider allow the HDO to review a recent third-party audit report that includes an assessment of the security controls and practices related to virtualization and separation of customer data?
   h. Do the service provider's customer registration processes provide an appropriate level of assurance based on the criticality and sensitivity of the information in the cloud service?
3. Patch and Vulnerability Management
   i. Is the service provider responsible for patching all components that make up the cloud service?
   j. Does the service provider's SLA include service levels for patch and vulnerability management that comprise a defined maximum exposure window?
   k. Does the HDO currently have an effective patch and vulnerability management process?
   l. Will the service provider allow the HDO to perform regular vulnerability assessments?
4. Encryption
   m. Does the service provider encrypt the information placed in the cloud service for both data at rest and in transit?
   n. Does the cloud service use only approved encryption protocols and algorithms (as defined in Federal Information Processing Standards 140-2)?
   o. Which party is responsible for managing the cryptographic keys?
   p. Are there separate keys for each customer?
5. Data Persistence
   q. Does the service provider have an auditable process for the secure sanitization of storage media before it is made available to another customer?
   r. Does the service provider have an auditable process for safe disposal or destruction of equipment and storage media (e.g., hard disk drives and backup tapes) containing customer data?

Integrity

Data integrity is the maintenance of data over its full lifecycle with the assurance it is accurate and consistent. The concept is a critical aspect of the design, implementation, and usage of any system which stores, processes, or transmits data.

1. Does the service provider provide data backup or archiving services as part of their standard service offering to protect against data loss or corruption?
2. How are data backup and archiving services provided?
3. Does the data backup or archiving service adhere to business requirements related to protection against data loss?
4. What level of granularity does the service provider offer for data restoration?
5. Does the service provider regularly perform test restores to ensure that data is recoverable from backup media?

Availability

The term "data availability" refers to the ability to ensure that required data is always accessible when and where needed.

1. Does the SLA include an expected and minimum availability performance percentage over a clearly defined period?
2. Does the SLA include defined, scheduled outage windows?
3. Does the service provider utilize protocols and technologies that can protect against distributed denial-of-service (DDoS) attacks?
4. Do the network services directly managed or subscribed to by the HDO provide sufficient levels of availability?
5. Do the network services directly managed, or subscribed to by the HDO provide an adequate level of redundancy/fault tolerance?
6. Do the network services directly managed, or subscribed to by the HDO provide an adequate level of bandwidth?
7. Is the latency between the HDO network(s) and the service provider's service at levels acceptable to achieve the desired user experience?

Incident Response and Management

1. Does the service provider have a formal incident response and management process with plans that clearly define how they detect and respond to information security incidents?
2. Does the service provider test and refine its incident response and management process and plans regularly?
3. Does the service provider's SLA clearly define the support they will provide to the HDO should an information security incident arise?
4. Does the service provider furnish enough information to enable the HDO to cooperate effectively with an investigation by a regulatory body?
5. Does the service provider›s incident response plan clearly define reporting requirements to meet regulatory requirements?

Maintaining a Continuous Monitoring Program

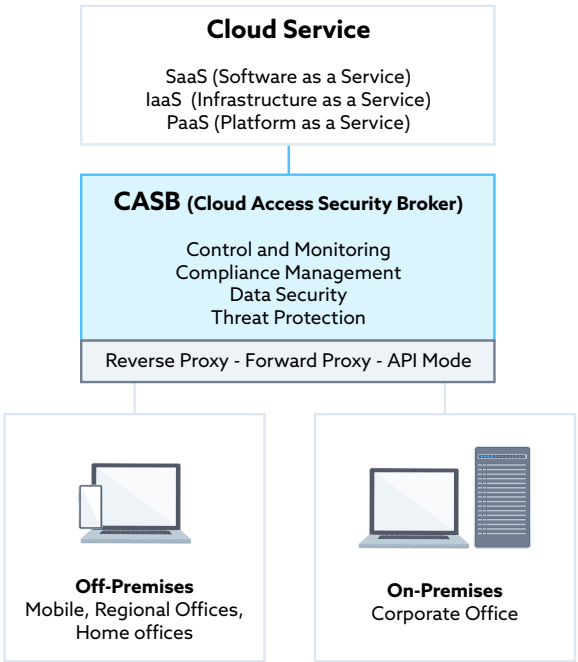
Establishing and implementing tools and controls within an information security, privacy, and compliance program is an essential part of any telehealth program. There is always a need for ongoing monitoring and management to ensure HDOs continue to enforce and enhance security operations. This is true for both internal controls as well as the information privacy and security programs utilized by the cloud service provider. Traditionally, this process is referenced as continuous monitoring. Continued monitoring helps ensure both the HDO and the cloud provider maintain the desired security posture (Herold, 2019).

Continuous monitoring activities are maintained throughout the full data, applications, and systems lifecycles, and should be tailored for continuous risk awareness and continuous compliance. Ongoing improvement initiatives ensure that cloud service provider security and privacy activities remain relevant and useful while providing metrics to gauge success and indicate where improvements are necessary. Selecting and implementing relevant metrics for the type of cloud services being provided help HDOs maintain an effective continuous monitoring program. The Cloud Security Alliance Security Trust and Assurance Registry (CSA STAR)—which is a registry of cloud providers that have met the security requirements and are certified—provides an open-source tool for annual assessments for continuous monitoring of security controls.

Another fundamental tool is a cloud access security broker. According to Gartner, «Cloud Access Security Brokers (CASB) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on.» (Gartner, 2019).

Cloud Access Security Brokers ensure HDOs understand what cloud connections are made and what data is sent to the cloud.

Finally, the Cloud Security Alliance Top Threats List is an annual compilation of the top cloud security threats. It can provide HDOs with further information on the concepts highlighted in this white paper. The CSA document includes business impacts for each threat, key takeaways, CSA security guidance, and the controls used to help mitigate the threats.



Conclusion

Currently, the COVID-19 response relies heavily on social distancing measures to fight the pandemic. For health care systems, telehealth has emerged as a critical technology for safe and efficient communications between health care providers and patients. According to a new World Health Organization (WHO) policy, telemedicine should be one of the alternative models for clinical services and clinical decision support (within the optimizing service delivery action). Additionally, the Centers for Medicare and Medicaid Services (CMS) has broadened access to Medicare telehealth services so that beneficiaries can receive an expanded range of services from their doctors without having to travel to a health care facility (HHS, 2020).

With the increased use of telehealth in the cloud, HDOs must adequately and proactively address data, privacy, and security issues. The HDO cannot leave this up to the cloud service provider, as it is a shared responsibility. The HDO must understand regulatory requirements as well as the technologies that support the system. Regulatory mandates may span multiple jurisdictions, and requirements may include both the GDPR and HIPAA. Armed with the right information, the HDO can implement and maintain a secure and robust telehealth program.

References

Aziz HA, Guled A, 2016. *Cloud Computing and Healthcare Services*. J Biosens Bioelectron 7: 220. doi: 10.4172/2155-6210.1000220

Bambauer, Derek E., 2013. *Privacy Versus Security*, The Journal of Criminal Law & Criminology Vol. 103, No. 3

Cloud Security Alliance, 2017. *Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*, Retrieved from https://cloudsecurityalliance.org/document/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v4-0/

Cloud Standards Customer Council, 2017. *Impact of Cloud Computing on Healthcare Version 2*.

Cloud Security Alliance, 2019. *The Egregious 11—Top Threats to Cloud Computing + Industry Insights*, Retrieved from https://cloudsecurityalliance.org/group/top-threats/

Gartner, November 2019. *Cloud Access Security Broker*, Retrieved from https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs

Herold Rebecca, 2019. *Continuous Oversight in the Cloud: How to Improve Cloud Security, Privacy and Compliance*. ISACA.

Joint Action to support the eHealth Network, 2017. *EU state of play on telemedicine services and uptake recommendations*.

Marcoux Rita M., and Vogenberg F. Randy, 2016. *Telehealth: Applications from a Legal and Regulatory Perspective, Pharmacy and Therapeutics* Vol 41 (9): P. 567–570. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5010268/

Mehraeen, Esmaeil & Ghazisaeedi, Marjan & Farzi, Jebraeil & Mirshekari, Saghar, 2016. *Security Challenges in Healthcare Cloud Computing: A Systematic Review*. Global Journal of Health Science. 9. 157. 10.5539/gjhs.v9n3p157.

National Institute of Standards and Technology, 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, Gaithersburg, MD. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

U.S. Department of Health & Human Services, 2003. *Summary of the HIPAA Security Rule*, Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

U.S. Department of Health & 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-notification-of-enforcement-discretion-for-telehealth-remote-communications-during-the-covid-19.html