Health Sector Coordinating Council
Cybersecurity Working Group

Manage Risks

Secure Medtech

Health Industry Cybersecurity -

Securing Telehealth and Telemedicine

OCTOBER 2023

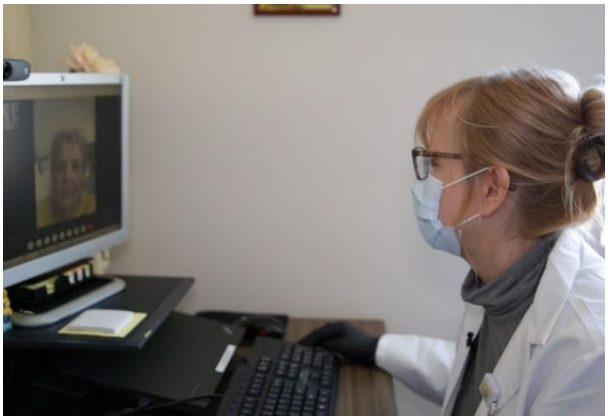
Reprint of 2021 Edition

Table of Contents

Introduction

Health care is increasingly moving to a digital platform. Recent major investments in health information technology, such as electronic health records and health information exchanges, have created enabling digital components that providers and vendors are leveraging for virtual health care services. These services are primarily delivered to those who otherwise cannot get them, such as those who live in America's most distant rural settings, the elderly, or patients at risk of contracting COVID-19 those who live in America's most distant rural settings.

Telehealth use has grown exponentially in response to COVID-19. FAIR Health research indicates 4,347% growth in telehealth claims to private insurers year-over-year, 2019-20.[1] As one example, one clinic chain had a 600% growth in telehealth in the first quarter of 2020 compared to the same time period a year before.[2] Additionally, Frost & Sullivan projects a 7-fold growth of telehealth by 2025.[3] The deployment of more mature analytics, better adherence to cybersecurity and privacy regulations, and the use of data to show return on investment are expected to maintain the drive of this significant telehealth expansion.[4]



Virtual health care service, such as telehealth, is now one of the fastest-growing areas in health care. The major expansion of telehealth during the pandemic as a vehicle to manage disrupted access is now being supported with long term support for the concept and decisions by the Centers for Medicare and Medicaid Services (CMS) and others to establish clinical reimbursement guidelines. Yet, this rapid expansion of telehealth services by a growing number of private and public providers comes during a time of enhanced cyber assault on the health care sector. These forces create the imperative to address the unique cyber security issues faced by clinicians, patients, and the systems in which they work.

The Health Sector Coordinating Council (HSCC) has developed this white paper, the "Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT)" guide,- for the benefit of health care systems, clinicians, vendors and service providers, and patients. All of these stakeholders share responsibility for ensuring that telehealth services achieve their optimum benefit with minimal risk to the privacy and security of the data, the consultations, and the systems hosting them.

---

1 https://www.fairhealth.org/states-by-the-numbers/telehealth

2 https://www.fiercehealthcare.com/payer/cvs-health-beats-wall-street-estimates-2b-profit-affirms-2020-earnings-guidance

3 https:/ww2.frost.com/news/press-releases/telehealth-to-experience-massive-growth-with-covid-19-pandemic-says-frost-sullivan/

4 Id. (Frost Report)

Indeed, the discipline of cybersecurity in a complex, connected environment like health care is multifaceted, requiring attention to cyber vulnerabilities and threats throughout the industry value chain. For this reason, the HSCC has developed a series of cybersecurity guidance documents that help health systems and their vendors and providers organize around this shared responsibility through various functional disciplines. Resources that supplement the HIC-STAT for managing health system cyber security include the Health Industry Cybersecurity Practices (HICP), the Health Industry Cybersecurity Supply Chain Risk Management (HIC-SCRiM) guide, and Managing Teleworking Security. These and many more are freely available for stakeholders in the healthcare community at https://healthsectorcouncil.org/hscc-recommendations/.

This white paper will review potential cybersecurity risks in the use and management of telehealth and telemedicine, and offer recommendations for addressing them. It will specifically focus on cybersecurity risks, regulatory issues, policies and procedures, audit tools, and best practices. As this is a rapidly evolving field with associated threat, the version of this document available on the website may be updated in the future.

About the Health Sector Coordinating Council Cybersecurity Working Group

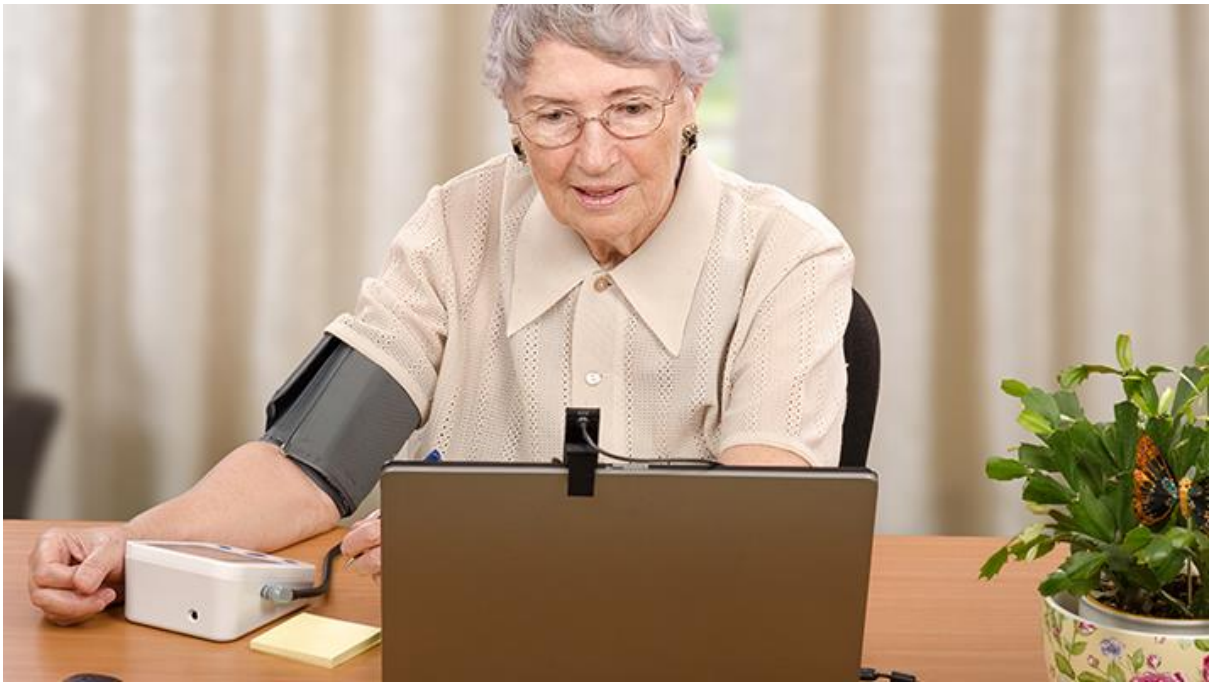
The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is the largest HSCC working group of more than 400 healthcare providers, pharmaceutical and medtech companies, payers and health IT entities partnering with government to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The CWG membership collaboratively develops and publishes freely-available healthcare cybersecurity best practices and policy recommendations, and produces outreach and communications programs emphasizing the imperative that cyber safety is patient safety.

What is Telehealth

The CMS defines telehealth as "the use of telecommunications and information technology (IT) to provide access to health assessment, diagnosis, intervention, consultation, supervision, and information across distance." Telehealth describes health technologies used to treat patients who are not in the same physical location as their provider, and includes clinician to clinician uses, for educational or consultative purposes. Telehealth encompasses the use of electronic and telecommunication technologies to support health care delivery, for both preventative and administrative activities.

Telemedicine, a subcategory of telehealth, refers to the use of remote clinical services, encompassing diagnosis, treatment, and monitoring. Telemedicine includes provider-to-provider consultations, telementoring and training (such as Project ECHO, which involves real-time collaborations via video technology between community providers and specialists at the Centers of Excellence), and direct provider-to-patient care, such as video-based telepsychiatry, which provides needed mental health care to patients for whom it may not otherwise be available.

Fueling telemedicine's emergence: are technological advancements that make it affordable and relatively easy to implement, the need to offer patients increased access to care due to geographic shortages, society's growing expectation for immediate availability of care, and the platform for data management that makes such care possible. Virtual care is optimal for patients who have limited mobility or who need complex long- or short-term care requiring a team approach, and who require specialists in areas where there are provider shortages, such as, for example, psychiatry.



Virtual care is available in three basic formats:

1. **Asynchronous** (store-and-forward video conferencing and imaging): the transmission of medical information to a qualified health care professional who assesses it offline, outside of real-time interactions.
2. **Synchronous** (live video and audio conferencing): real-time communication between the patient and qualified health care professional, typically telehealth.
3. **Remote patient monitoring (RPM)**: patients or care providers use mobile devices and technology to transmit patients' health data to a health care professional who will assess the data using special telehealth computer systems or specialty software applications installed on computers, smartphones, or tablets.

A REACH Healthcare Foundation survey revealed that telemedicine adoption in 2017 was slow, finding that 37% of acute care hospitals, 70% of primary care providers, and 90% of skilled nursing facilities had no telemedicine program. This low uptake was attributed to inconsistent reimbursement, a narrow scope of clinical services, and state-based legal barriers, even as telemedicine services were available across the clinical platform in hospitals, physician practices, skilled nursing facilities, pharmacies, psychiatric facilities, and correctional facilities. At that

time, telemedicine's five top specialty applications were stroke, psychiatry, neurology, radiology, and pediatrics.[5] Radiology had been using virtual reading for more than 10 years. Though not included in the Reach Survey, telemedicine use for ICU patient management within and between hospitals has also become a mainstream clinical and operational service. The REACH survey also reported 83% of health care executives were likely to invest in telemedicine and telehealth.[6]

Since the start of the pandemic in late winter of 2020, all of these venues have seen a dramatic and sustained growth in these services, with strong support and advocacy by organizations such as the American Hospital Association (https://www.aha.org/telehealth) and the American Telemedicine Association (https://www.americantelemed.org).

Associated Cybersecurity Risk

Expanding use of remote technology in healthcare, including for telehealth and telemedicine, has been accompanied by a substantial increase in connectivity and exposure. According to a recent study by SecurityScorecard and DarkOwl LLC, the rapid adoption and onboarding of telehealth vendors has led to a significantly increased digital footprint and attack surface, leaving both provider and patient data at risk.[7]

Consequently, hackers and criminal groups are able to exploit these vulnerabilities and easily infiltrate a network for financial gain or operational disruption. For example, in 2020 according to the study, telehealth providers have experienced a nearly exponential increase in targeted attacks as popularity skyrocketed.

- 117% increase in website/IP malware security alerts
- 65% increase in security patching of known vulnerabilities
- 56% increase in endpoint vulnerabilities that enable data theft
- 16% increase in patient-accessed web application vulnerabilities
- 42% increase in file transfer protocol vulnerabilities that expose information travelling between a client and a server on a network
- 27% increase in remote desktop protocol security issues given the widespread adoption of remote work

Healthcare is now also facing greater problems with requirements for user authorization, authentication, and accountability - all of which are also common issues for other industries such as banking. Because telemedicine and telehealth involve the collection and transmission of personal health information (PHI) and personally identifiable information (PII), they inadvertently present hackers with extremely valuable targets.

5 https://www.healthlawinformer.com/wp-content/uploads/2017/05/2017-telemed-us-industry-survey.pdf

6 https://www.healthlawinformer.com/wp-content/uploads/2017/05/2017-telemed-us-industry-survey.pdf

7 Listening to Patient Data Security: Healthcare Industry and Telehealth Cybersecurity Risks

For more information about how to deal with these and other vulnerabilities, see the HSCC Health Industry Cybersecurity Practices (HICP).

Why is Telehealth a Target in Cyberspace?

First, telehealth and telemedicine are, simply, ***easy targets***, particularly because of:

- data traversing network/Internet access (typical vulnerabilities associated with data in motion);
- integration of many networks/technologies means no unified security policy/implementation and no central governance, rendering system security dependent on the weakest link. By its very nature, much telehealth communication needs to travel outside of controllable environments (e.g. to patients' personal devices).

Second, they are ***valuable targets***, because:

- PII and PHI can command a high price on the black market.

Finally, they are ***plentiful targets***, as evidenced by the fact that:

- per Research2Guidance 2017 mHealth Economics report[8], 325,000 mobile health apps are currently in existence;
- the global medical device connectivity market is expected to exceed $2.5B by 2024.

What Are the Major Types of Attacks Against Telehealth Systems?

Common threats to and impacts on telehealth systems can include:

Compromise of Confidentiality

- Theft of PII or PII
- Credential harvesting
- Data exfiltration

Compromise of Integrity

- Exploitation of financial transaction system
- Manipulation of clinical data

Compromise of Availability

- Ransomware
- Denial of Service

8 Research2Guidance 2017 mHealth Economics report.

Policy Underpinnings of Healthcare Cybersecurity

The prevailing federal law governing privacy and security for healthcare in the U.S. is the Health Insurance Portability and Accountability Act (HIPAA) which was signed into law in 1996. The Act mandates data security and privacy controls to keep medical information safe. The Department of Health and Human Services (HHS) publishes the HIPAA Privacy Rule, the HIPAA Security Rule, and the HIPAA Breach Notification Rule.

The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information.

The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" (i.e., health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards) must put in place to secure individuals' "electronic protected health information" (e-PHI). The Security Rule requires administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information. HIPAA business associates are directly liable for their own violations of the HIPAA Rules including applicable provisions of the Security Rule. OCR fact sheet details BA HIPAA liability (https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html).

Finally, the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Within

HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil monetary penalties.

In 2009, the American Recovery and Reinvestment Act (ARRA) included the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH was created to incentivize the healthcare providers' and business associates' adoption of health information technologies, particularly electronic health records (EHR) / electronic medical records (EMR) technology. "Meaningful use," as it became called, required HIPAA cover entities and business associates to demonstrate their use of certified EHR technology to improve the quality of healthcare. HITECH also created stricter enforcement of the Breach Notification, Privacy and Security Rules of HIPAA by mandating audits for covered entities. These audits are to ensure that HIPAA covered entities and business associates comply with their obligations under the HIPAA Rules.

Further, the HITECH Act established what is generally known as the Breach Notification Rule, requiring that covered entities, within 60 days of discovery, report to HHS, affected individuals, and the media, any breaches of unsecured health information affecting 500 or more individuals. Smaller breaches are to be reported to HHS annually. Data breaches of information that is protected by methodologies that render it unusable, unreadable, or indecipherable (e.g., encryption) are exempt from the notification requirement.

The Cybersecurity Information Sharing Act (CISA) of 2015 established a mechanism for cybersecurity information sharing among private-sector and federal government entities. It provides safe harbors from liability for private entities that share cybersecurity information, and authorizes entities (outside the federal Government) to monitor systems and take precautionary cybersecurity measures. The Act is designed to bolster federal cybersecurity protections, including the assessment of the federal government's cybersecurity workforce, and implement measures to improve cybersecurity preparedness of critical information systems and networks. Within this Act is Section 405(d), which aims to improve cybersecurity in the healthcare industry, and includes several sub-sections that call for the creation of reports, task forces, and security approaches. Section 405(d) resulted in the creation of a public-private task group, organized under the Health Sector Coordinating's Joint Cybersecurity Working Group, which developed healthcare cybersecurity best practices called the "Health Industry Cybersecurity Practices (HICP)". This resource offers to health providers a set of cybersecurity best practices that should be used in the protection of telehealth and telemedicine systems and services.

In January of 2021, H.R. 7898 was enacted into law as P.L. 116-321, which amended the HITECH Act to directed OCR, when implementing a compliance audit and imposition of fines in the wake of a covered entity breach, to consider the extent to which the covered entity maintained certain recognized security practices, such as the NIST Cybersecurity Framework, the HSCC Health Industry Cybersecurity Practices and others.

During the COVID-19 national emergency, OCR issued a notice that it would exercise enforcement discretion and not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency. It is unclear as of this writing the extent to which this may become permanent.

Depending on legal or geographic factors, other regulations may need to be considered for the telehealth infrastructure as whole or in part, for example, Payment Card Industry Data Security Standard (PCI-DSS), Sarbanes-Oxley, or State-specific cybersecurity and privacy laws (e.g., California CCPA, Massachusetts 201 CMR 17, or Texas HB300).

Regulations and Organizational Policy

Federal and state regulations have not kept in step with the rapid and widespread adoption of telehealth technologies across the country. Over the past several years, states have begun to modernize their rules around telehealth with most taking on the fundamentals of defining telehealth roles, geographic requirements, basic definitions, and coverage and reimbursement terms.

Most states have not developed extensive guidance with respect to security criteria for telehealth programs and technologies. In a review of several articles published between 2008-2016 that focus on security and privacy considerations in the use of telehealth, there does not seem to be consensus about the use and disclosure of PHI in telehealth. Some health systems will allow sharing with certain groups as part of their privacy policy while other systems may be more restrictive about sharing PHI. HIPAA stipulates that proper authorizations are warranted when there are requests for information, and an accounting of disclosures is necessary when PHI is shared. However, there remains uncertainty as to what parts, if any, of the telehealth session will be saved, for how long, how they will be maintained, and where they will be stored.

If the telehealth sessions are recorded and kept with the electronic health record (EHR) then proper authorizations are necessary when PHI is requested. However, there is no standard method for how this is done. Some systems may convene a telehealth session and not store any of the information that was transmitted. Some may record the session but then destroy the recording after the session is over. Some may record and store the session or even transmit the session to a third party for additional treatment and consultation.

Currently, there is no single federal agency with authority to establish and enforce privacy and security requirements for the entire telehealth ecosystem. At a minimum, telehealth systems need to maintain security and privacy consistent with those of all other forms of care. In considering the end-to-end telehealth service, along with processes needed to provide that service, providers must apply the HIPAA Privacy and Security Rules. Providers may choose to vary standards or requirements according to their own unique circumstances as long as they are not in direct conflict with HIPAA.

- In telehealth delivery models involving provider-to-provider communication, the entities at both ends are typically required by HIPAA to implement appropriate security safeguards, such as end user authentication and data protection, including data encryption measures. However, in telehealth models where one end of the communication is the patient, that endpoint falls outside the controlled and supervised environment of a HIPAA-regulated clinical care setting. As a result, there may be security and/or privacy issues or gaps about the patient's use of the technology that need to be identified and addressed. This provides opportunity for industry leadership in best practices and market-driven technology features to protect telehealth interactions.
- If a telehealth technology qualifies as a medical device, the FDA may also be engaged via its regulatory authority over the device manufacturer, through either its Premarket Guidance for the integration of security features in a device or its Postmarket Guidance for managing or supporting the security of a device deployed in a clinical environment. The FDA does not directly address privacy issues but focuses on security to the extent that it affects medical device safety and effectiveness.

Cybersecurity Considerations

Cybersecurity risk areas associated with the supply chain need to be considered when evaluating telehealth solutions: choosing the technology to be used, designing patient experience and workflows, and handling data. For more information about managing risk from technology vendors and service providers, see the HSCC Health Industry Cybersecurity Supply Chain Risk Management (HIC-SCRiM) guide, which provides detailed guidance elaborating on the following concepts.

Technology Procurement and Deployment – As we consider the risk that telehealth technology solutions may bring, overarching concerns exist that speak to the process of technology and vendor evaluation. Within the provider environment, management should establish a well-defined process to address the scope of a technology procurement project and how it will be deployed and managed from end to end. Through an established process, even an informal one, solutions and vendors need to be vetted by those best able to assess these risks.

It can also help to ensure enterprise security requirements are included in the proposed solutions and that key stakeholders across the organization are engaged, providing stakeholders visibility into the process and an opportunity to contribute to technology/vendor selection.

As with any selection process, research the technology considered; the specific technology/vendor should be chosen based on reliable external recommendations (such as industry reports, peer organization recommendations, and/or referrals). Reputable industry and market research publications may also help identify alternatives and guide the ultimate selection of a final vendor solution.

Technology/solution assessment should also include adequate clinical administrative and security testing prior to use. Planning for patching, updates, and end of life technology must be proactive. Attention to the maintenance and updating, including software patching, of legacy systems, will be required to protect both the specific system and the entire IT ecosystem. For more guidance about managing legacy systems, please see the upcoming HSCC publication - "Health Industry Cybersecurity – Managing Legacy Technology (HIC-MaLT)".

Technology Availability and Resiliency – Consideration should be given to the prospect of system failure and shutdown, especially at a time of increased outside cyber intrusions. Alternative solutions must be considered. Depending on the volume and intended use cases, a backup or temporary alternative may or may not be practical. If feasible, a backup/recovery process should be established, maintained and tested periodically. For guidance about responding to and operating during and after a cyber security attack see, the HSCC Health Industry Cybersecurity Tactical Crisis Response (HIC-TCR) Guide or ASPR TRACIE"s "Healthcare System Cybersecurity: Readiness and Response Considerations"

Technology Monitoring and Troubleshooting – Continuous monitoring of the technology on which the solution is based should be part of the operational plan. The capability to monitor for any security-related events would include, for example, system configuration changes and changes to administrator accounts and/or privileges. Ideally, any monitoring should be as close to real time as possible.

End User Management - As we shift the focus from the technology, several patient/end user controls and session-specific risks need to be addressed that are tied directly to the patient/end user:

End User Training and Awareness – Depending on the type of technology and the complexity of the solution being implemented, patient end users will need at least some basic instruction and usage guidelines. Lack of proper training and guidance may result in unintended consequences such as inappropriate access and improper disclosure of information.

End User Access and Credentials – The patient/end user should be required to provide unique credentials to access the solution. The provider should establish a well-defined, simple and standardized process to verify the identity of the patient, including unique identifiers as part of the agreement between the provider and patient. As the patient may have varying levels of technology experience, accommodations should be made to facilitate the usability of any on-boarding process.

Verification and validation of patient end user tools and configuration – Everyone using the portal is an entry point, and potential vulnerability, to the system. Patients, families, and others utilizing the system should be encouraged to use secure internet options, preferably from their home. This preference would apply regardless of whether they're using a laptop, tablet, phone, or other device. Regardless of how this is accomplished, all communications should be encrypted and patients provided instruction about the importance and process for protecting their data and the system.

User/Event Activity monitoring – For this type of a solution, the ability to monitor select types of critical events and activities associated with the end user is important. For example, all privileged user/administrator access should be logged and monitored to help protect the integrity and confidentiality of the system and data, if applicable.

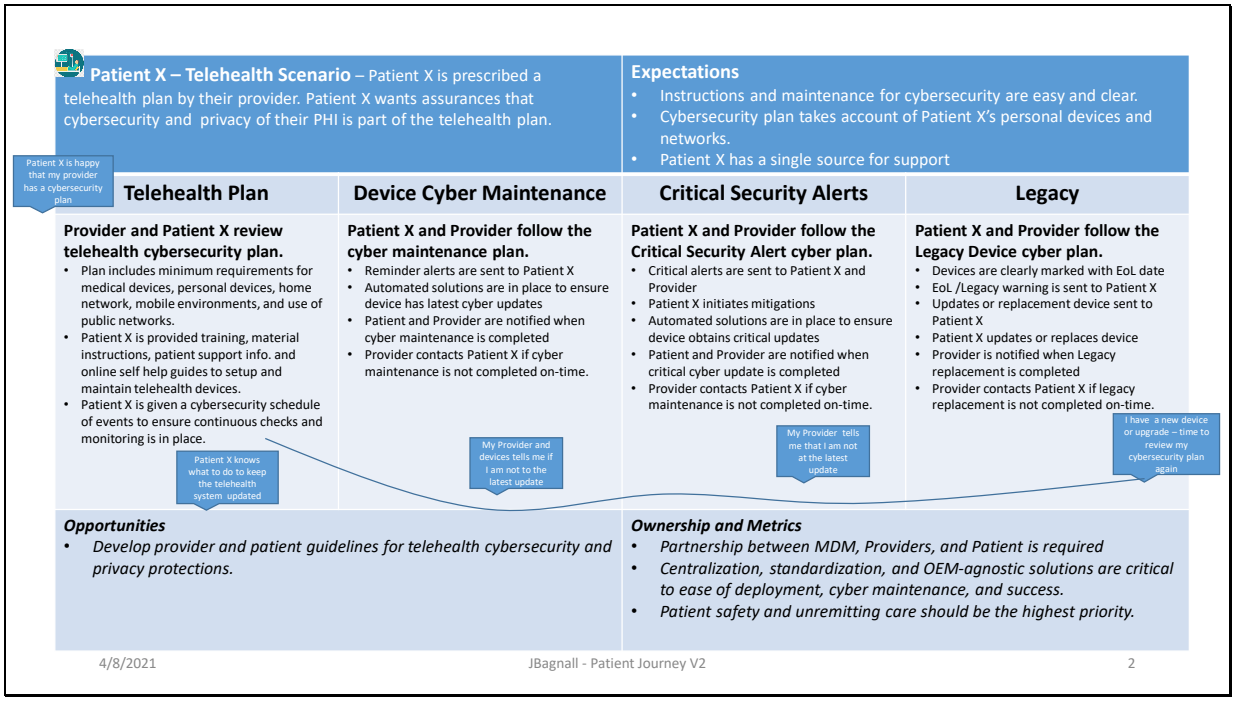
Data Risks and Controls - Finally, the risks and controls to the data should be evaluated, with consideration given to:

- appropriate confidentiality protections according to the type of data that will be used, shared, and managed in conjunction with using a digital health solution;
- requirements of the solution or process for any exchange of PII or PHI between the physician/provider and the patient end user. Specifically, the way the information will be exchanged (i.e., verbally, electronically via an application, both verbally and electronically, etc.) needs to be clearly defined;
- how such information will be protected, such as leveraging encryption for data at rest (strongly recommended for end user devices or data stored in cloud services) and end-to-end encryption for data in transit (rather than relying on security of the individual segments like WIFI, TLS, etc.)
- the need and capability to protect any data that needs to be shared electronically in addition to general user guidelines for the provider and patient. This requires determining how this data will be handled once exchanged, i.e., written in patient's file, or input into EMR/EHR application.

Any new processes introduced into the healthcare ecosystem should bring benefits to the patient and practitioner alike. Now, more than ever, security should be designed into the implementation of a well-balanced telehealth system to avoid unnecessary risks to patients and patient data.

Table 1 below summarizes an aspirational use case for involving patients and clinicians in cybersecurity awareness and procedures related to the use of telehealth.

Considerations for non-clinical environments (Telehealth Vulnerability Management)



Telemedicine Cyber-Guidance: Cybersecurity Capabilities and Audit/Compliance Assessment Options

Cybersecurity is critical to the telehealth business and enables protection of the IT systems and data used to provide telemedicine services. The security capabilities and auditability are also required when dealing with patient data. Providers of telehealth services should implement and maintain appropriate security measures.

Assumptions

1. The following security related capabilities will help keep the IT system environments secure and support audits and forensics activities.
2. The company delivering telehealth services should have good basic identity management capabilities, which manage and audit employees from onboarding to changing roles and access rights to offboarding ("joiners, movers, and leavers").
3. The company delivering telehealth services should have a program and process in place that implements and maintains effective network, systems, and data security measures to support these services. Minimum security capabilities and audit support the following:

Asset management

- Identify the current environments used to deliver telehealth functionality and store any related data (what PCs, desktops, servers, databases, or other infrastructure used to deliver telemedicine services)
- Identify the versions and patch levels of the operating systems, software, firmware, and applications in the environment.

Endpoint Protection

- For systems used to provide the telehealth services (such as PCs, desktops, workstations, laptops, etc.), implement tools that identify and protect against malicious software, such as malware or viruses

Logging and Monitoring Capabilities

- Systems should record information related to activities. Logs of noteworthy activities and events could include, but not be limited to, the following:
  - Identity Management logs (who accessed the environment and when)
  - Infrastructure change logs (e.g. changes or upgrades to servers, network components, software applications, databases, etc.)
  - Database logs (related to data access and changes, especially for PHI and PII)
  - Application access logs (who has access to a particular application, what activities they performed, any security violations or system errors).

Encryption Capabilities

- Encryption of data at rest and in transit is an "addressable implementation specification" under the Security Rule, meaning that HIPAA-covered entities are expected to implement it unless it is not "reasonable and appropriate" to do so.
- Encryption capabilities should include the following specific items:
  - Encrypt the end-to-end communication channel between providers as well as between provider and patient.
  - Ensure integration with any system is secure and encrypted where required (e.g., EHR/EMR, pharmacy systems, financial or billing systems, etc.)
  - PHI or GDPR data are encrypted in transit and, where feasible, at rest

Email Encryption

- Any scheduling or follow-up communication associated with telehealth services should be encrypted
  Note: For any encryption solution, access to the underlying encryption system should be logged, audited, and limited to only authorized system administrators.

Mobile Device / Wireless Security

- Since many devices today rely on mobile devices and/or wireless network access for connectivity, consideration needs to be given to securing the devices used in a telehealth session as well as the data intended to be shared between providers and between patient and provider.

Data Loss Prevention Tools

- Helps ensure sensitive data management by identifying and tracking movement and usage

Advanced Logging Capabilities

- Central repository for all logging (e.g., access logs, network logs, database logs)
- Tools to provide advanced analytics, identification and alerting for abnormal behavior
- Advanced forensics capability

Privileged Account Management

- Tools to provide the capability to manage, secure and audit privileged account activities and events.

Security Incident Response

- Solutions and/or services that help with identifying and responding to security-related vulnerabilities and incidents. For recommendations about effectively communicating with patients about security vulnerabilities and incidents, see the HSCC white paper on Vulnerability Communications available in the 3rd quarter of 2021 at https://healthsectorcouncil.org/hscc-recommendations/.

Ways to Assess or Evaluate Telemedicine Solutions

Periodic Security Assessments - Security assessment is a systematic evaluation of the security of information systems by measuring how well it conforms to a set of established criteria. A thorough assessment typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices. Security assessments are measured against established criteria, such as information technology or security policies and standards, or widely used security frameworks.

Security assessments may also include an assessment of security vulnerabilities, which includes detecting and classifying weaknesses in information systems, networks, and software applications. Good telehealth security management requires the use of vulnerability scanning tools, which are essential to help identify, evaluate, prioritize, remediate, manage, and report on vulnerabilities.

A security assessment may also consist of penetration testing, the process of identifying security vulnerabilities in a system using various techniques typically used by real-world security hackers or fraudsters. Such penetration tests actively attempt to exploit weaknesses in an environment and require various levels of expertise and tools. Such testing can help determine if the current security measures and defenses are sufficient, and if not, identify areas for improvement.

Implementing and Maintaining a Telemedicine Program

Numerous cybersecurity issues must be addressed when designing a telemedicine program to ensure effective overall information and cyber security. An organization must consider relevant Federal and state compliance requirements and develop a strategy to address current and emerging security threats. Additionally, an organization should

consider the necessary infrastructure partners, equipment partners, workforce partners, and external partners who can implement and maintain such a program.

The telemedicine program's technologies may incorporate elements of standalone solutions or various mobile health (mHealth) applications. Security concerns overlap these categories.

A telemedicine program comprises three main constituents: the payer, the provider or health system, and the telemedicine service provider. Each must ensure the security of their portion of the program. Each must establish an effective cybersecurity program that can protect the systems that process or store the related health data. These programs should also align with a security framework (such as the National Institute of Standards and Technology [NIST] Cybersecurity Framework) as well as the HSCC HICP (which aligns to the NIST CSF), and include implementation of cybersecurity best practices.

Telehealth technologies typically fall into three categories:

1. **Remote Patient Monitoring (RPM) devices, which include:**
    - Wearables such as smartwatches or wristbands to monitor and communicate vital signs
    - Canes and walkers to detect and alert when a patient falls
    - Stationary chairside/bedside devices to monitor patient vital signs

Each monitoring solution generally comprises four components:

- Sensors
- Local data storage repository
- Central repository
- Diagnostic software/applications

RPM security is required for endpoint devices at a patient's residence, including:

- Home routers and systems
- Applications and devices
- Self-monitoring/self-testing
- Monitoring patient health and clinical information at a distance
- Evolving home-based therapies like home dialysis or home infusion.

Health care delivery organizations are responsible for the security of their interna infrastructure, including:

- Routers, switches, hubs, and access points
- Servers, applications, interfaces, and insider threats

2. **Real-time audio/video communication**
    - Real-time access to providers for patients living away from population centers
    - Triage between general practitioners and high-priority treatment facilities
    - Collaboration of multidisciplinary health professionals located in different areas
    - Cellular devices (smartphones, tablets, and other mobile sensors) and networks
    - Wifi, Bluetooth, SMS, MMS, QR codes, and GPS

3. Store-and-forward technologies, including:
    - Provider transmission of information or images such as MRIs, X-rays, photos, and pre-recorded videos

Vulnerabilities are associated with:

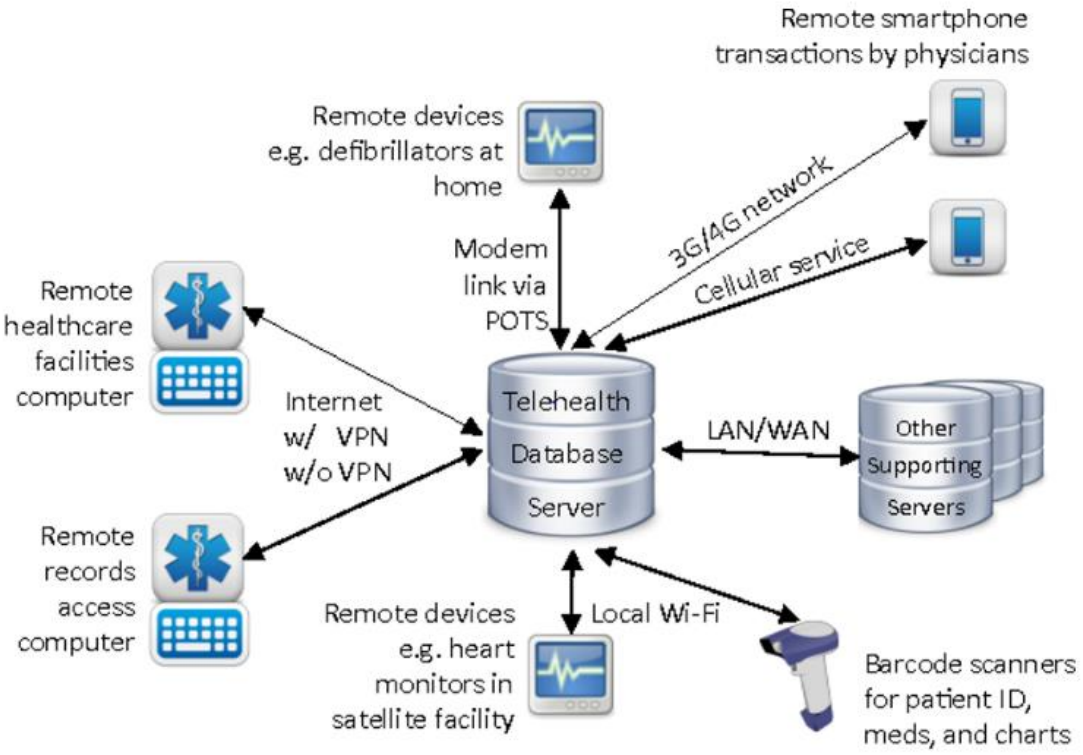
- Storage—internal, directly attached storage, network storage, and removable drives
- Apps/programs and interfaces

Cybersecurity Best Practices

Organizations should make cybersecurity a bedrock principle. Efforts should focus on closing threat windows and minimizing surfaces vulnerable to attack. This is best accomplished by acting quickly to reduce the number of vulnerable accessible systems. The defense should be built as quickly as possible after the threat is discovered.

Board Governance and Senior Level Buy-In – Senior leadership should support initial and ongoing investments in the cybersecurity program to ensure information is safeguarded to the highest degree possible.

24/7 Security Operations Center (SOC) – Cybercriminals launch cybersecurity threats to disrupt capabilities and compromise data around the clock, which requires, resources allowing, an in-house or out-sourced SOC that is staffed 24/7 by trained employees who are dedicated to tracking and addressing threats. By doing so rapidly, an organization can reduce its threat window and systems risk.



Typical telehealth information network

Threat Intelligence Sharing – Entities in the same ecosystem will often experience the same cyberattacks. Advanced notice of new threats allows organizations to build effective defenses to prevent the proliferation of attacks against their infrastructure, so participating in threat intelligence programs and proactively sharing information with the Health Information Sharing and Analysis Center, governmental bodies, private sector partners, and downstream business associates/vendors is a key way to remain alert to developing threats.

Ongoing Automation and Manual Tests – Because cybersecurity risks constantly evolve, pressure testing systems to ensure the system's safety, reliability, and leak resistance is key. This is best accomplished by using a combination of ongoing automated and manual tests. Testing should leverage real-time attack signatures that reflect the evolving threat landscape. Pressure testing allows an organization to better identify and address existing vulnerabilities, reducing the overall attack surface.

Employee Training – Continuous workforce training, testing, and education will help ensure employees can identify current threats. Beyond the typical annual HIPAA security and privacy training, organizations must train their workforce to identify and report security threats. Examples of trainings include spear phishing campaigns, social engineering tests, and security breach simulations, which should be run regularly to develop a responsive and engaged workforce.

Future of Telehealth Security

The trend toward the consumerization of information technologies into corporate environments is continuing. This has included increased reliance on mobile devices and applications, while expanding consumer use of Wi-Fi, Bluetooth technologies, QR codes and GPS. This trend is also having a meaningful impact on how patient care and information is provided. There will be continued growth of opportunities in telehealth to leverage new and existing technologies in more creative and complex ways to enhance how care is provided. As a result, it will be incumbent upon providers to design appropriate security measures and accountabilities while offering these services in the future. This ever-changing environment makes it even more critical that effective security measures and controls be designed into these new solutions and processes during the earliest stages of project planning and design. Subsequently, ongoing activities such as vulnerability management, change management, and event monitoring will help to ensure those security measures are maintained effectively over time.

The application of artificial intelligence (AI) will offer use cases that can be applied to telehealth solutions. While AI will present opportunities for providing more sophisticated and effective telehealth solutions, a potential drawback to utilizing AI is it will likely draw the attention of new and creative cyberattacks. Such developments may prompt additional security measures such as advanced authentication methods or other security measures designed specifically to protect AI-based solutions.

Today, AI providers are typically not the telehealth providers themselves, but instead third parties. This places the burden on telehealth providers to vet and secure these AI-based solutions.

Review of Cybersecurity Oversight and Best Practices

Federal oversight is limited to elements of telehealth, such as devices to capture patient vital signs and other physiologic data; information storage for the encounter; and the technology to establish a connection, view, and exchange information. The Office for Civil Rights governs the handling of protected health information (PHI) that is handled by covered entities, predominantly providers, along with their business associates. Security rules within HIPAA are also limited and place the onus for monitoring and modulating the efficacy of security practices on providers. The U.S. Food and Drug Administration (FDA) may regulate the safety and efficacy of certain medical devices used in telehealth services; however, they have issued guidance only, and not regulation, regarding management of cybersecurity controls for medical devices. Some have called for the Federal Trade Commission (FTC) to provide increased oversight for telehealth transactions and in protection of consumers.

However, in the absence of oversight, there is opportunity for industry stakeholders to develop best practices and create market pressures for these practices to take hold. Through the CISA 405(d) task groups, for example, health care entities have developed several guidance documents and toolkits to ensure cybersecurity hygiene and monitoring in health care settings. Some examples which can be applied across organizations and to provider telehealth services are included as follows.

- The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) provides 10 key cybersecurity practices organized by the top five current threats. This toolkit is an ever-evolving set of guidelines for health care providers of varying sizes and sophistication to adopt policies and practices that conform to market security standards and provide organizations with a level of assurance that they are not outliers with respect to their cybersecurity practices. For a notable use of this structure, please see the Klas-Chime white paper "How Aligned are Provider Organizations with the Health Industry Cybersecurity Practices Guidelines?"
- The Medical Device and Health IT Joint Security Plan (JSP) outlines a framework and recommendations for medical device security, including the use of Internet Protocol (IP) address and network segments. The JSP provides device manufacturers and vendors with a framework for developing baked-in cybersecurity features into their devices, maintaining security throughout the lifecycle of a device, including determining when to retire devices, and communicating with customers on cybersecurity threats and vulnerabilities. The JSP also provides a script for providers to internalize in their communications with their device manufacturers and vendors.
- The Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook provides a framework for health delivery organizations and other stakeholders to plan for and respond to cybersecurity incidents around medical devices, ensure effectiveness of devices, and protect patient safety.

Appendix

For technical audience

RMP Security Concerns

Environment	Concern
Patient's Residence or Other Originating Site	To secure home routers: use technology which includes appropriate encryption technologies, restrict guest networks, disable SSID broadcasting, maintain and protect strong, difficult-to-guess passwords, etc. Secure all devices on the home network, even those not related to telehealth services, to prevent them from being used as an internal hop point. This includes: • Patching • Anti-virus protection • Usage of Virtual Private Networks (VPNs) • Usage of personal firewall • Ensuring all configurations balance security with functionality Ensure all telehealth-specific devices are secured in accordance with vendor recommendations, always apply industry best practices, and remain persistent about updates.
Intermediary Information Transport	Protections, countermeasures, and remediation • Traffic monitoring, intrusion detection services • Prevention of IP spoofing and distributed denial of service (DDoS) attacks • Blacklisting known malicious sites • Malware detection
Healthcare Delivery Organization (HDO)	Protections, countermeasures, and remediation: • Ensure compliance with FDA medical device cybersecurity regulations: https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm Collaborate with ISPs • DDoS • Phishing campaigns • Blacklisting Inform patients • Ensure they are aware of all FDA recommendations/requirements applicable to their telehealth applications and devices • Provider cybersecurity guidance as resources allow

	• Develop standard operating procedures for frequently used patient telehealth devices and applications, distribute accordingly Apply defense-in-depth, principle of least privilege and weakest-link approaches to overall cybersecurity posture. This includes: • Network access control – ensuring no unauthorized access points exist on network • Firewall implementation/administration • Intrusion detection/prevention services • Endpoint security, including anti-ransomware services • Compliance reporting to HHS all PHI/ePHI breaches • Static and dynamic application security/testing

Store and Forward – Security/Mitigations

Technology Category	Concern
Storage Devices (Internal device storage, directly attached storage, network attached storage, removable drives)	• Patching • Anti-virus protection • Use of Virtual Private Networks (VPNs) • Use of personal firewall • Ensuring all configurations balance security with functionality
Transmission Technologies (ISP, Satellite, Cellular)	• Encryption • Network access control • Firewalls • Intrusion detection/prevention services
Interfaces (Hardware, apps/programs)	• Firmware and software updates • Secure code development

Real-Time Audio/Video – Security/Mitigation

Considerations	Details
Challenges	Balance between transmission time and security: • Speed is critical • More overhead = more data to pass = slower Transmission protocols • TCP v. UDP • RTP (real-time transport protocol)

	• Real-time Control Protocol (RTCP) • WebRTC • Websockets • HTTP/2 Encryption algorithms • IPSec • SSL/TLS1.2
Types of Attacks	• Man-in-the-middle attack • Timing attack • Truncation attack • Downgrade attack • Padding-oracle attack

Technical Articles Related to Cybersecurity Best Practices:

"Toward secure and privacy-preserving data sharing in e-health systems via consortium blockchain"

- https://www.ncbi.nlm.nih.gov/pubmed/29956061

"Cryptanalysis and improvement of a biometrics-based authentication and key agreement scheme for multi-server environments."

- https://www.ncbi.nlm.nih.gov/pubmed/29534085

"Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems."

- https://www.ncbi.nlm.nih.gov/pubmed/29477428

Resources:

- National Cybersecurity Center of Excellence Securing Telehealth Remote Patient Monitoring System
  - https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth
- Center for connected health policy:
  - https://www.cchpca.org/
  - The CCHP is a non-profit working to advance telehealth initiatives. They released the following report that details state-by-state regulations for telemedicine, some of which contain references to cybersecurity
    - https://www.cchpca.org/sites/default/files/2019-05/cchp_report_MASTER_spring_2019_FINAL.pdf
- American Telemedicine Association: https://www.americantelemed.org/
- Center for Telehealth and e-health Law: https://ctel.org/
- Northeast Telehealth Resource Center: https://netrc.org/

State Regulations:

California *(which apply to other states too if they have Californian patients)*. California has the most specific guidelines of any state that arguably go beyond HIPAA and HITECH regulations. In 2018, the state of California enacted the California Consumer Privacy Act of 2018 (CCPA), into law. The CCPA is the nation's strictest consumer privacy and data protection measure affecting any for-profit healthcare company doing business in California. The European Union General Data Protection Regulation (GDPR) is the only other legal enactment which rivals CCPA, and there are several areas where CCPA requirements are more specific than those of the GDPR.

The law specifically applies to organizations that (1) collect the personal information (PI) of California Residents (either solely or jointly with others), and (2) either (i) exceed $25 million in annual gross revenues; (ii) annually transacts in the PI of 50,000 or more consumers, households, or devices; or (iii) derives half or more of its annual revenues from PI sales. This will apply to any business that collects, uses, or shares personal information of California residents, including businesses that are outside the state for temporary or transitory purposes.

PI is defined as any information that could reasonably be linked to a consumer, including but not limited to personal identifiers, commercial information, biometric information, Internet activity information and employment information. CCPA excludes, the sale of information from or to a consumer reporting agency (so long as information is used as part of a consumer report and in compliance with the Fair Credit Reporting Act), and information that is collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act or the Driver's Privacy Protection Act to the extent that CCPA is in conflict with either law. CCPA states that it "shall not apply to protected or health information that is collected by a covered entity governed by the [California] Confidentiality of Medical Information Act [the CMIA]…or governed by the privacy, security, and breach notification rules…established pursuant to the Health Insurance Portability and Accountability Act of 1996. For purposes of [the CCPA], the definition of 'medical information' in the [CMIA] shall apply and the definitions of 'protected health information' and 'covered entity' from the federal privacy rule shall apply." Thus, companies regulated under either the CMIA or HIPAA should continue complying with those rules, as defined by the CMIA, or protected health information, as defined by HIPAA, as CCPA does not supersede those laws.

CCPA places requirements on those covered businesses to ensure consumer rights and related notices that resemble the European Union's General Data Protection Regulation (GDPR). CCPA's rights include: the Right of Access, Right of Deletion, Right to Know, and the Right of Equal Service. Violations of those provisions may be prosecuted by the California attorney general via the state's Unfair Competition Law (UCL). In addition to UCL penalties, the law allows civil penalties. CCPA also provides a limited private right of action for data breaches in which unencrypted PI is subject to unauthorized access and is exfiltrated or otherwise disclosed as a result of a violation of the business's duty to observe reasonable security procedures and practices.

The following are examples of state telehealth security laws and requirements that organizations should consider when contemplating security regulations. In most cases, when care is delivered across state lines, providers must follow the laws and rules of both states.

State Telehealth Cybersecurity Laws and Requirements (as of April 2021)

(Unless otherwise indicated, all information comes from the Center for Connected Health Policy https://www.cchpca.org/telehealth-policy/current-state-laws-and-reimbursement-policies)

District of Columbia:

- Medicaid will only reimburse for telemedicine if providers develop protocols that govern the:
  - Provider's compliance with the security and privacy requirements of the Health Insurance Portability and Accountability Act of 1996, approved August 21, 1996 (110 Stat. 1936; 42 U.S.C. Section 1320d et seq.).

Delaware:

- Provider must implement confidentiality protocols that comply with all HIPAA requirements and include, but are not limited to:
  - All telemedicine transmissions must be performed on a dedicated secure line or must use an acceptable method of encryption which protects the confidentiality and integrity of the information being transmitted
  - Specifying the individuals who have access to electronic records
  - Usage of unique passwords or identifiers for each employee or other person with access to the client records
  - Ensuring a system to prevent unauthorized access, particularly via the internet
  - Ensuring a system to routinely track and permanently record access to such electronic medical information
  - Ensuring that both the originating site and distant site are secure, private locations which protect the confidentiality of the client and the telecommunications exchanged between the two sites
  - These protocols and guidelines must be available for inspection at the telemedicine site and to Domain Mapping (DMAP) upon request

Kentucky:

- The Cabinet is required to do the following:
  - Develop policies and procedures to ensure the proper use and security for telehealth, including but not limited to confidentiality and data integrity, privacy and security, informed consent privileging and credentialing, reimbursement and technology.

Louisiana:

- "Louisiana Telehealth Access Act," found at: La. R.S. 40:1223.1 et seq.
- Applicable language from a provision of this statute states:
  - §1223.4. Telehealth; rulemaking required
    - Each state agency or professional or occupational licensing board or commission that regulates the practice of a healthcare provider, as defined in this Part, may promulgate, in accordance with the Administrative Procedure Act, any rules necessary to provide for, promote, and regulate the use of telehealth in the delivery of healthcare services within the scope of practice regulated by the licensing entity. However, any rules and regulations shall be consistent with and no more restrictive than the provisions contained in this Section.
  - The rules shall, at a minimum, provide for all of the following:

    - Application of all laws regarding the confidentiality of healthcare information and the patient's rights to the patient's medical information created during telehealth interactions.
    - Application of the same standard of care by a healthcare provider as if the healthcare services were provided in person.
    - Licensing or registration of out-of-state healthcare providers who seek to furnish healthcare services via telehealth to persons at originating sites in Louisiana. The rules shall ensure that any such healthcare provider possesses, at a minimum, an unrestricted and unencumbered license in good standing to perform the healthcare service in the state in which the healthcare provider is located, and that the license is comparable to its corresponding license in Louisiana as determined by the respective Louisiana licensing agency, board, or commission
    - Each state agency and professional or occupational licensing board or commission is authorized to provide by rule for a reasonable fee for the license or registration provided for in this Subsection
    - Exemption from the telehealth license or registration required by this Subsection for the consultation of a healthcare professional licensed by this state with an out-of-state peer professional.
  - Nothing in this Part shall be construed to authorize a state agency or professional or occupational licensing board or commission to expand, diminish, or alter the scope of practice of any healthcare provider.

- Louisiana also has the "Database Security Breach Notification Law," which is the general Louisiana HIPAA breach law that applies to all data breaches – found at La. R.S. 51:3071 et seq. A summary of this law can be found here: https://nuemd.com/hipaa/breach-guide/LA.html
- Under this general law, the following definition applies:
  - A "breach of the security of the system" is the "the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person." (R.S. 51:3073(2))
  - In June 2016, the governor signed into law, HB 570, (the "Act"), eliminating the prior requirement that physicians practicing telemedicine maintain an office in Louisiana or contract with in-state providers. The Act also changes the telemedicine modality required for a patient encounter from "two-way video" technology to "interactive audio" (provided the modality is sufficient to meet the same standard of care as an in-person encounter). The Act requires telemedicine providers make referrals to, or arrangements for, follow-up care when necessary. This law also grants boards, commissions, and other authorities the ability to promulgate new rules and regulations that are consistent with this law, but no more restrictive than the statute itself.

- Some highlights of the Act include:
  - Telemedicine. "Telehealth" remains defined as a mode of delivering healthcare services that utilizes information and communication technologies to enable the diagnosis, consultation, treatment, education, care management, and self-management of patients at a distance from healthcare providers. Telehealth allows services to be accessed when providers are in a distant site and patients are in the

originating site. Telehealth facilitates patient self-management and caregiver support for patients and includes synchronous interactions and asynchronous store and forward transfers.

- Standard of Care. The standard of care remains the same as if the healthcare services were provided in person. A healthcare provider may utilize interactive audio without the requirement of video if, after accessing and reviewing the patient's medical records, the provider determines he or she is able to meet the same standard of care as if the healthcare services were provided in-person.
- Physician Licensure. A provider practicing telemedicine must hold an unrestricted license to practice medicine in Louisiana or a telemedicine special license in Louisiana.
- Remote Prescribing. The Act did not alter existing requirements or standards for remote prescribing.
- Disclosures. The Act did not alter existing requirements or standards for disclosures. Under current board rules, prior to providing telemedicine services, a physician must disclose to the patient: 1) the name, Louisiana medical license number and contact information of the physician, 2) the physician's specialty or area of practice, 3) how to receive follow-up and emergency care; 4) how to obtain copies of medical records and/or ensure transmission to another medical provider; 5) how to receive care in the event of a technology or equipment failure; and 6) notification of privacy practices.
- Informed Consent. The Act did not alter existing requirements or standards for informed consent. Under current board rules, a physician must notify a patient of the relationship between the physician and patient and the respective role of any other health care provider with respect to management of the patient and that the patient may decline to receive medical services by telemedicine at any time.
- Patient Records. The Act added that a physician practicing telemedicine must create a medical record on each patient and make such record available to the board upon request. As before, a physician practicing telemedicine must document the telemedicine services rendered in the patient's medical records according to the same standard as that required for non-telemedicine services. Medical records including, but not limited to, video, audio, electronic, or other records generated as a result of providing telemedicine services are considered confidential and are subject to all applicable state and federal laws and regulations relative to the privacy of health information.
- Venue. Venue in any suit filed involving care rendered via telehealth pursuant to these laws must be instituted before the district court of the judicial district in which the patient resides or in the district court having jurisdiction in the parish where the patient was physically located during the provision of the telemedicine service. The patient is considered physically located at the originating site.

Nebraska:

- https://www.securetelehealth.com/medicaid-reimbursement/68.html
- According to the Nebraska HHS Finance and Support Manual:
  - All confidentiality laws and other requirements that apply to written medical records shall apply to electronic medical records, including the actual transmission of the service and any recordings made during the time of the transmission.
  - All transmissions must be performed on a dedicated secure line or must use an acceptable method of encryption adequate to protect the confidentiality and integrity of the transmission information. Transmissions must employ acceptable authentication and identification procedures by both the sender and the receiver.

New Mexico:

- Managed Care Organizations must:
  - Follow accepted HIPAA and 42 CFR part two regulations that affect telemedicine transmission, including but not limited to staff and contract provider training, room setup, security of transmission lines, etc; the MCO shall have and implement policies and procedures that follow all federal and state security and procedure guidelines.

New York:

- The New York State Department of Health advises that all services delivered via telehealth must be performed on dedicated secure transmission linkages that meet the minimum federal and state requirements including, but not limited to 45 CFR Parts 160 and 164 (HIPAA Security Rules); 42 CFR Part 2, New York State Public Health Law Article 27-F, and New York Mental Hygiene Law §33.13. Transmissions must employ acceptable authentication and identification procedures by both the sender and receiver. In addition, New York State notes that HIPAA requires that a written business associate agreement, or contract that provides for privacy and security of PHI, be in place between the telehealth provider and the supporting telehealth vendor.
- Section 899-a of the New York State General Business Law also requires businesses to secure the "private information" of New York State residents. The security provisions are largely similar to those in the HIPAA Security Rule. Private information is defined to include any personal information concerning a natural person in combination with a specific data element, such as social security number or account number, and biometric information and username/email address.

Oklahoma:

- Eligible sites for live video: The medical or behavioral health related service must be provided at an appropriate site for the delivery of telehealth services. An appropriate telehealth site is one that has the proper security measures in place; the appropriate administrative, physical, and technical safeguards should be in place that ensures the confidentiality, integrity, and security of electronic protected health information. The location of the room for the encounter at both ends should ensure comfort, privacy, and confidentiality. Both visual and audio privacy are important, placement and selection of the rooms should consider this. Appropriate telehealth equipment and networks must be used considering factors such as appropriate screen size, resolution, and security. Providers and/or members may provide or receive telehealth services outside of Oklahoma when medically necessary.

Texas:

- Security requirements
  - The software system used by the distant site provider must allow secure authentication of the distant site provider and the client.
  - All client health information generated or used during a telehealth or telemedicine medical service must be stored by the distant site provider in a client health record. If the distant site provider stores the patient health information in an electronic health record, the provider should use software that complies with the Health Insurance Portability and Accountability Act (HIPAA) confidentiality and data

encryption requirements, as well as with the United States Department of Health and Human Services (HHS) rules implementing HIPAA.

- Any telemedicine program must provide written protocols, policies, and procedures to the HHS commission that address, among other things, system security, including the integrity of information that is collected, program integrity, and system integrity.

Utah:

- Telehealth services must meet industry security and privacy standards, including compliance with HIPAA and the federal Health Information Technology for Economic and Clinical Health (HITECH) Act
- If a hospital participates in telemedicine, it shall develop and implement policies governing the practice of telemedicine in accordance with the scope and practice of the hospital. These policies shall address security, access, and retention of telemetric data, and define the privileging of all health professionals who participate in telemedicine.

Selection of Relevant Regulations and Security Standards

Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Privacy Rule, Security Rule, Breach Notification Rule – Defines Protected Health Information (PHI); Regulations for use, security, and disclosure of PHI, and notification of breaches; 18 identifiers
Cybersecurity Information Sharing Act of 2015 (CISA)	Section 405: Improving Cybersecurity in the Healthcare Industry – Requires collaboration by HHS with other healthcare industry stakeholders (both government and private sector) to share.
Federal Information Security Management Act of 2002 (FISMA)	Defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats.
Federal Risk and Authorization Management Program (FedRAMP)	A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP enables Agencies to rapidly adapt from old, insecure legacy IT to mission-enabling, secure, and cost-effective cloud-based IT.
Federal Trade Commission Act of 1914	Section 5 is used to monitor and regulate confidentiality of mHealth devices
NIST Draft Securing Telehealth Remote Patient Monitoring Ecosystem	Guidance/Reference for security and privacy risks to telehealth and remote patient monitoring implementations
NIST Special Publication 1800-1: Securing Electronic Health Records on Mobile Devices	Key components: architecture, implementation recommendations, standards/controls, and risk assessment and outcomes.

[1] https://www.fairhealth.org/states-by-the-numbers/telehealth

[2] https://www.fiercehealthcare.com/payer/cvs-health-beats-wall-street-estimates-2b-profit-affirms-2020-earnings-guidance

[3] https:/ww2.frost.com/news/press-releases/telehealth-to-experience-massive-growth-with-covid-19-pandemic-says-frost-sullivan/

[4] Id. (Frost Report)

[5] https://healthitsecurity.com/news/covid-19-impact-on-ransomware-threats-healthcare-cybersecurity

Acknowledgments

The Health Sector Coordinating Council wish to express its gratitude to the many member representatives who worked on the Telemedicine Task Group and contributed significant hours and thought leadership to the development this resource. Some individuals listed have changed affiliations since the first publication.

In particular, we wish to thank:

Mark Jarrett
Chair
Northwell Health

Penny Chase
MITRE

Stephen Collins
Midland Memorial

Steve Hyland
Cardinal Health

Robert Jarrin
Consultant

Till Jolly
HHS

Nimi Ocholi
Medtronic

Reuven Pasternak
DHS

Vito Sardanopoli
US Imaging Network

MacLanahan Stevens
Spok

Christine Sublett
Sublett Consulting

Zeynep Sumer-King
Greater NY Hospital Association

Sean Whitney
Anthem

Margie Zuk
MITRE