ManageEngine
IT Security

Cybersecurity in telehealth:
A strategic guide for **CISOs in healthcare**

Introduction

Telehealth refers to the use of digital communication technologies to deliver healthcare services, support clinical practices, and facilitate patient education and health management remotely.

It encompasses a broad range of services, including live video consultations, remote patient monitoring (RPM), mobile health (mHealth) applications, and asynchronous communication like email or app-based messaging between patients and healthcare providers.

According to the Telehealth Global Market Report 2025, the telehealth market size is projected to be $227.18 billion by the end of 2025, and is expected to reach $558.31 billion in 2029 with a CAGR of 25.2%. While the COVID-19 pandemic may have been the catalyst for the widespread adoption of telemedicine and telehealth as a whole, the convenience and quality of care it offers is the reason for its continued growth. A 2024 Deloitte survey found that 24% of respondents were ready to switch providers for continued access to virtual health options. But, as telehealth adoption grows, the cybersecurity risks it poses do too. Each digital interaction in the realm of telehealth expands the attack surface and potential vulnerabilities that threat actors can exploit. Ensuring data integrity, confidentiality, and compliance across these technologies is critical for CISOs and healthcare security leaders.

Key takeaways for CISOs

Telehealth has become a cornerstone of modern healthcare delivery, offering operational agility, improved patient access, and scalability. However, its growing adoption also introduces new dimensions of risk and responsibility for CISOs.

1. Increased attack surface:

As telehealth extends care beyond traditional clinical settings, it brings a proliferation of connected devices, apps, and virtual endpoints. Each of these become a potential entry point for cyberthreats, making robust identity and access management, endpoint protection, and encrypted communications non-negotiable.

2. Data privacy and compliance pressures:

Virtual consultations and remote monitoring generate sensitive PHI across cloud platforms, mobile apps, and wearables. Ensuring HIPAA compliance, maintaining audit trails, and securing data in transit and at rest are vital to prevent breaches and regulatory penalties.

3. Need for secure remote infrastructure:

Telehealth relies heavily on VPNs, secure APIs, and cloud-hosted services. CISOs must ensure secure configurations, Zero Trust architecture, and continuous monitoring to defend against misconfigurations, insider threats, and credential-based attacks.

4. Incident response across distributed environments:

The decentralized nature of telehealth demands a reimagined incident response strategy. Threat detection, log correlation, and response coordination must work across networks, third-party apps, and hybrid cloud environments.

5. Building patient trust through security:

Data breaches can erode patient confidence and disrupt patient care. Proactively improving the organization's security posture and demonstrating transparency builds digital trust in virtual care environments. CISOs must play a pivotal role in aligning security architecture with telehealth expansion to protect patient data, enable safe innovation, and support the digital evolution of care delivery.

What are the key components of telehealth?

Telehealth is a transformative approach to healthcare that leverages technology to improve accessibility, efficiency, and patient engagement. Its key components include:

Live (synchronous) video communication

Enables real-time interactions between patients and healthcare providers using video conferencing tools. This is commonly used for routine checkups, specialist consultations, or follow-up appointments. For example, patients from rural places may use Zoom to consult with their cardiologist about their pain symptoms, next steps of care, or prescription refills.

Store-and-forward (asynchronous) technology

Health data, such as images, test results, and medical history, is collected, stored, and sent to a healthcare provider for later evaluation. This is especially helpful in the case of specialties like dermatology, radiology, and pathology. For example, a general practitioner in a remote clinic may send high-resolution photos of a patient's skin lesion to a dermatologist for review.

RPM

Patients use wearable or connected (IoT) medical devices, such as blood pressure cuffs or glucose monitors, to collect and transmit health data to clinicians. This is especially beneficial for chronic disease management. For example, diabetic patients may wear a continuous glucose monitor that alerts their diabetologist whenever their glucose levels spike or drops alarmingly.

mHealth

These are health-related apps on smartphones or tablets that help patients manage their health through reminders, fitness tracking, medication management, or symptom monitoring. For example, a medication reminder app like Medisafe notifies patients to take their prescribed pills on time or alerts them when a refill is required.

Why is telehealth important?

Telehealth has enabled the delivery of clinical and non-clinical services remotely. Its importance lies not only in improving access to care but also in enhancing the quality, efficiency, and resilience of healthcare systems.

Improved access to care:

Telehealth bridges geographic gaps by reaching patients in rural, underserved, or mobility-restricted settings. It enables timely consultations with specialists, mental health providers, and primary care physicians, regardless of location.

Continuity of care:

Telehealth ensures uninterrupted patient care when in-person visits become restricted due to natural disasters or other emergencies. It also supports long-term management of chronic diseases through regular virtual check-ins and monitoring.

Cost efficiency:

Telehealth reduces overhead and travel costs for both patients and healthcare providers. It lowers emergency room visits and hospital re-admissions through proactive remote interventions and follow-ups.

Convenience and patient engagement:

Patients can consult healthcare professionals from the comfort of their homes, leading to higher appointment adherence and satisfaction. Digital tools, such as mobile apps and wearables, encourage self-monitoring and active participation in care plans.

Workforce optimization:

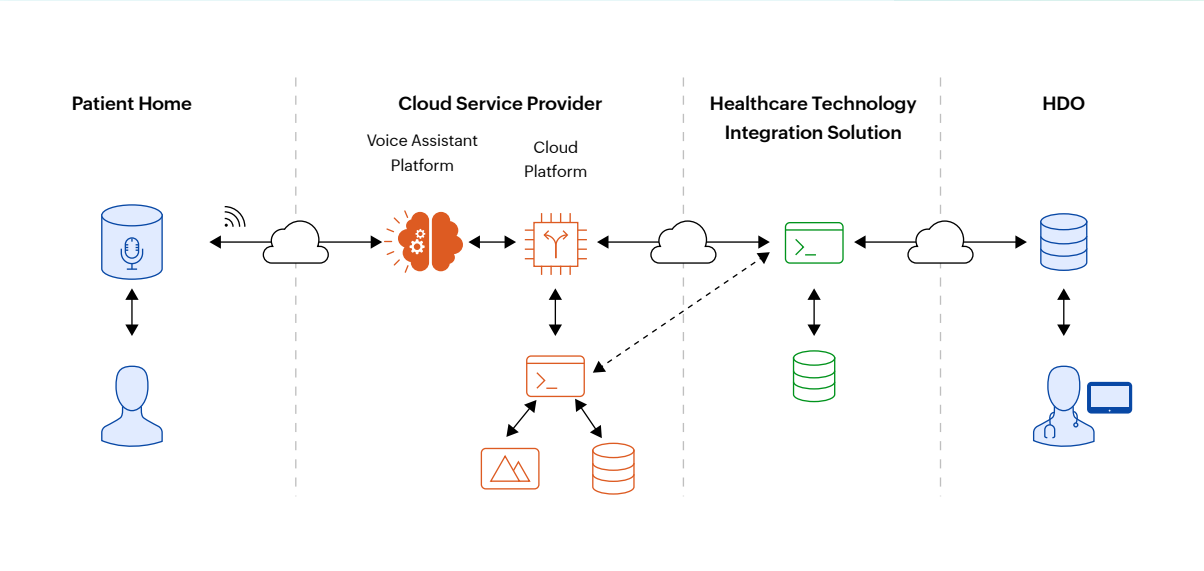
Telehealth helps providers manage higher caseloads more efficiently. It supports remote collaboration among specialists and enables healthcare organizations to allocate resources more effectively across regions.

Support for public health and prevention:

Remote care delivery helps monitor population health trends, support vaccination campaigns, provide mental health support, and educate communities, all while minimizing physical contact.

How does telehealth work?

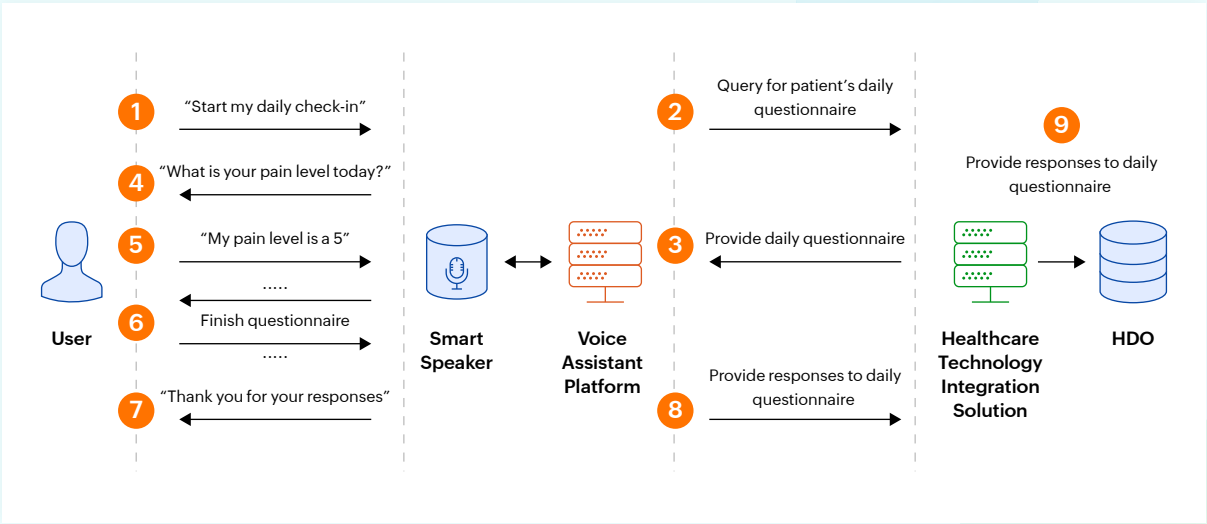
Telehealth operates by using secure digital communication technologies to deliver healthcare services remotely. It connects patients and healthcare providers through a combination of internet-enabled devices, cloud-based platforms, and real-time or asynchronous communication tools. A high-level architecture of how patients use smart speakers to interface with patient information systems or healthcare information systems, as depicted in the NCCoE/NIST report, Mitigating Cybersecurity Risk in Telehealth Smart Home Integration, is shown below.



(Image source: NCCoE/NIST report)

Figure 1: High-level architecture of telehealth smart home integration.

As observed in Fig. 1, there are four domains that facilitate telehealth smart home integration: the patient home, cloud service provider, a healthcare technology integration solution, and healthcare delivery organizations (HDOs). The patient, having Wi-Fi connectivity and a smart home device with the ability to accept voice commands (like a smart speaker), will issue a request to it; for example, to start their daily check-in. The cloud service provider has a voice assistance platform that will receive the patient's request. It will then use natural language processing to use the voice input to trigger the application logic that establishes a network session with the patient information system. The healthcare technology integration solution is the one that enables patient interaction with HDOs and patient information systems. The HDOs will host patient information and clinical systems, patient portals, electronic records, and other systems. Fig. 2 shows how a patient's request to start their daily check-in will operate.

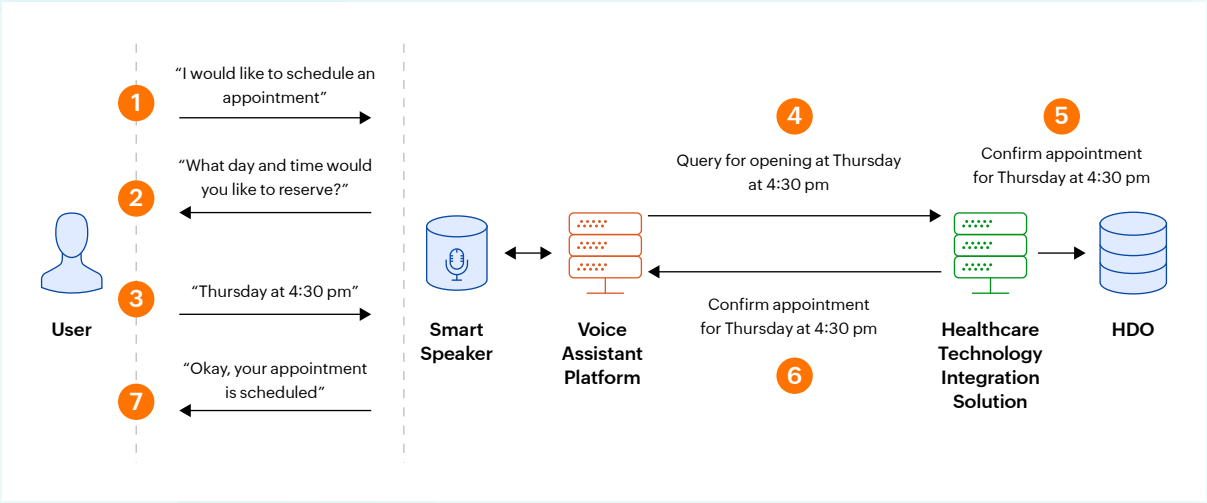


(Image source: NCCoE/NIST report)

Figure 2: How a patient regimen check-in works.

1. Patient access and initiation:

Patients use a telehealth platform, such as a mobile app, patient portal, or web interface, to schedule appointments (see Fig. 3), get prescription refills, access medical records, or initiate virtual consultations.



(Image source: NCCoE/NIST report)

Figure 3: Patient scheduling an appointment by leveraging telehealth Smart Home integration.

2. Digital communication and data exchange:

Depending on the service, it can involve live-video conferencing, store-and-forward technology, or RPM tools.

3. Integration with electronic health records (EHRs):

The telehealth system often integrates with the provider's EHR to ensure seamless access to patient history, medication lists, and prior diagnostics, facilitating informed decision-making.

4. Clinical decision and care delivery:

Healthcare providers assess the data from the RPM tools, communicate diagnoses, prescribe medications electronically, or recommend further in-person visits if needed.

5. Follow-up and patient engagement:

After the consultation, the telehealth platform may send follow-up instructions, medication reminders, or educational materials. Patients can also use chatbots or message portals to ask further questions.

What are the privacy and security challenges in telehealth?

As telehealth becomes a central component of modern healthcare delivery, it introduces new vectors for cyber risk. This includes privacy challenges arising from environmental factors such as lack of private space for vulnerable populations (e.g., homeless, elderly, or adolescents), difficulty sharing sensitive health information remotely; operational factors such as reimbursement, payer denials, technology accessibility and/or digital literacy, training and education about telehealth platforms; and data security issues. However, addressing the environmental and operational factors that put telehealth users at risk is beyond the scope of this book.

Here are the privacy and security challenges associated with telehealth platforms:

1.

Data transmission vulnerabilities

What it means: Telehealth involves transferring electronic protected health information (ePHI) across networks which are often public or not sufficiently secure.

Why it's a risk: Without end-to-end encryption (E2EE) or secure protocols like TLS, data packets can be intercepted in transit through manipulator-in-the-middle attacks. This exposes sensitive patient details like diagnoses, prescriptions, and personal identifiers.

Example: A provider uses an unsecured Wi-Fi connection for a video consult, enabling an attacker to eavesdrop or capture the session data.

2. Device and endpoint insecurity

What it means: Both patients and clinicians often use personal smartphones, tablets, or laptops, and these devices may not always be managed or patched regularly.

Why it's a risk: Unpatched vulnerabilities, lack of anti-malware software, or absence of firewalls make these endpoints susceptible to exploits, which threat actors can use as entry points into healthcare networks.

Example: A keylogger on a nurse's personal tablet captures login credentials to the telehealth portal.

3. Lack of standardized security protocols

What it means: During the pandemic-driven telehealth surge, many new vendors entered the market, and healthcare organizations adopted diverse platforms.

Why it's a risk: Not all platforms are HIPAA or GDPR compliant. Some may lack secure storage, encrypted messaging, or identity verification.

Example: A telehealth app with hardcoded admin credentials or no session timeout leads to a breach that exposes thousands of patient records.

4. Insider threats and misuse

What it means: Insider risks come from both malicious intent and human error; they can be caused by hospital staff or trusted third-party vendors.

Why it's a risk: Over-privileged access, lack of role-based access control (RBAC), and inadequate session monitoring can allow insiders to misuse patient data without immediate detection.

Example: Out of curiosity, a billing staff member accesses the mental health notes of a celebrity. Viewing this data is not relevant to their role, thus violating privacy norms.

5. Ransomware and malware attacks

What it means: With RPM devices and telehealth smart home integration, there's a drastic increase in the attack surface. This, in addition to the sensitive ePHI and PII that may be shared with the provider, makes it a high-value ransomware target.

Why it's a risk: Ransomware can halt critical care delivery, block access to teleconsultation systems, or threaten to leak sensitive medical data.

Example: A ransomware attack on a hospital's telehealth backend causes canceled appointments, data exfiltration, and legal repercussions.

6. Third-party vendor risks

What it means: Telehealth platforms often depend on APIs, cloud services, video conferencing tools, and EHR integrations.

Why it's a risk: A vulnerability in one third-party component (e.g., video SDK) can cascade into the entire ecosystem.

Example: A breach in a third-party transcription service exposes thousands of doctor-patient conversations.

7. User authentication weaknesses

What it means: Weak passwords, reused credentials, or a lack of multi-factor authentication (MFA) may be common across patient and provider accounts.

Why it's a risk: Inadequate user authentication allows account takeover, impersonation, and unauthorized record access.

Example: A hacker logs into a patient's telehealth account to view medical history, current diagnosis, treatment plans, and prescriptions due to reused credentials from another breach.

8. Compliance and regulatory gaps

What it means: Global compliance mandates such as HIPAA, the GDPR, and India's DPDP Act are complex, and each impose strict requirements on data processing and storage. A summary of the HIPAA guidelines on telemedicine is shown below:

Guideline	Description
Conduct an audit	If an organization is unaware of how healthcare professionals communicate with patients, it is impossible ensure compliance.
Analyze risks	The risk analysis required by the HIPAA Security Rule should extended to uses and disclosures of PHI during remote communications.
Develop policies	Policies that already exist for face-to-face interactions with patients should be extended to cover remote interactions with patients.
Business Associate Agreements	Include any third parties who provide telemedicine services on the organization's behalf if no direct treatment relationship exists.
Verification procedures	Ensure business associates report all security incidents (as required by §164.314) to know when access credentials have been compromised.
Record consent	Consent is advised when a requested channel of communication is unsecure or when there is a risk of a consultation being overheard.
Document and retain documentation	Some, but not all, telemedicine platforms automatically record remote communications with patients and archive them securely.

(Source: The HIPAA Journal)

Why it's a risk: Non-compliant platforms risk fines, data breaches, and reputational loss.

Example: A U.S.-based provider uses a foreign telehealth platform that stores data outside U.S. jurisdiction without consent, violating HIPAA data residency rules.

9. Inadequate audit trails and monitoring

What it means: Many telehealth systems lack centralized logging or SIEM integrations for real-time monitoring.

Why it's a risk: Suspicious behaviors like credential sharing or off-hours access may go undetected, increasing the duration a threat remains undetected.

Example: An attacker uses compromised credentials for weeks before being noticed, accessing hundreds of patient files.

10. Patient privacy concerns

What it means: Patients may not fully understand how their data is collected, shared, or monetized by telehealth platforms.

Why it's a risk: Opaque privacy policies, lack of consent mechanisms, and behavioral tracking erode patient trust and may violate data protection regulations.

Example: A telehealth app shares usage analytics with third-parties without patient knowledge, violating the GDPR's transparency principle.

Ensuring cybersecurity in telehealth: Best practices

Ensuring cybersecurity in telehealth requires a layered, proactive approach that blends technical safeguards, governance, and continuous vigilance.

Implement E2EE for telehealth communications

Protecting sensitive patient data with E2EE during transmission between patient and provider is critical. Telehealth platforms must use strong encryption protocols like TLS 1.3 or AES-256 for video, audio, messaging, and file transfers. Audit regularly to ensure that encryption is properly implemented and maintained.

Enforce strong authentication and access controls

Weak authentication is a leading cause of healthcare breaches. Mandate MFA for all users, including patients, providers, and administrative staff. Coupled with RBAC, this ensures users only access what they need, preventing unnecessary data exposures. It's important to regularly review and revoke unnecessary or outdated privileges, especially for temporary staff or contractors.

Conduct vendor risk management and due diligence

Telehealth platforms often rely on third-party services (e.g., cloud, EHR integration, video APIs), thus expanding external risks. So, make sure you evaluate all vendors for compliance with HIPAA, the GDPR, and other required data protection regulations. Ask the vendors for security certifications like SOC 2 Type II or ISO 27001, and embed breach notification clauses in contracts. Maintain a vendor risk register and conduct annual audits of critical service providers.

Secure endpoint devices used in telehealth

End-user devices, especially in BYOD environments, are common targets. Enforce mobile device management policies to secure mobile and desktop platforms and enable disk encryption, automatic software and patch updates, remote wipe, and anti-malware on all endpoints. Offer hardened, organization-approved telehealth devices for providers handling high-risk data.

Establish a secure, compliant cloud architecture

With telehealth heavily reliant on cloud infrastructure, misconfigurations can expose sensitive data. Use cloud security posture management to enforce best practices and monitor changes. Segregate workloads and enforce the principles of least privilege, Zero Trust, and other IAM core standards. Store data in regions aligned with legal and regulatory requirements.

Ensure continuous monitoring and logging with SIEM solutions

Real-time threat visibility reduces the time threats remain undetected. Integrate telehealth systems with your SIEM and enable detailed logging of sessions and access patterns. Leverage user and entity behavior analytics (UEBA) to detect anomalies like credential abuse or suspicious login patterns. SIEM also offers DLP and CASB capabilities, or at least allows integration with such tools. This can help you monitor and control access to telehealth platforms and other cloud applications, and prevent ePHI from being downloaded to personal devices. The SOAR capabilities in a SIEM can help with automatic response workflow execution.

Develop an incident response plan specific to telehealth

Standard incident response plans often overlook telehealth-specific scenarios. Create tailored playbooks for ransomware, credential compromise, and data leaks in clinical workflows. Conduct tabletop exercises with clinical, IT, and compliance teams, and include telehealth vendors to validate readiness and coordination.

Conduct regular security awareness training

Even with technical controls, human error remains a top risk. Train healthcare staff and providers on phishing, secure communication, and proper data handling. Educate patients on identifying fake apps and safe login practices. Keep training role-based and scenario-driven to make it actionable and memorable.

Implement data minimization and retention policies

Over-collection and prolonged storage of PHI increases both breach risk and compliance issues. Define data retention limits based on clinical need and billing requirements. Use automated tools to purge outdated data and ensure policies align with HIPAA and other local regulations.

Ensure compliance through regular risk assessments

The threat and regulatory landscape is constantly evolving. Conduct regular risk assessments specific to telehealth systems and workflows. Prioritize remediation of identified issues and validate your program against standards like NIST CSF, the HITRUST CSF, or ISO 27799 to demonstrate due diligence.

Related solutions

ManageEngine
AD360

ManageEngine AD360 is a unified IAM solution that provides SSO, adaptive MFA, UBA-driven analytics, and RBAC. Manage employees' digital identities and implement the principles of least privilege with AD360.

To learn more,

Sign up for a personalized demo

ManageEngine
Log360

ManageEngine Log360 is a unified SIEM solution with UEBA, DLP, CASB, and dark web monitoring capabilities. Secure hybrid cloud infrastructure and get audit-ready reports for HIPAA, the GDPR, and NIST CSF with Log360.

To learn more,

Sign up for a personalized demo