TITLE: **Telehealth Policy for Providers, Home Care, and Pharmacies**		
DEPARTMENT:		
Effective Date:	**Revised Date:**	**Next Review Date:**
Prepared by:		**Date:**
Administrative Approval: Chief Executive Officer, Chief Information Security/Privacy/Compliance Officer		
CEO:		Date:
CISO:		Date:
PO/CO:		Date:
All other related polices/procedures/protocols: User Access, Acceptable Use, Mobile Device, Security Management, BAA, Training		

SEE LAST PAGE FOR REVIEW HISTORY

Purpose:

To establish procedures enabling {residents/patients} to receive health care services via the use of electronic information and remote telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, and public health and health administration.

Scope and Applicability

This policy, associated procedures and guidelines apply to Workforce Members that provide health care services to {patients/residents} and to health care providers authorized to perform telehealth services to <CLIENT> {patients/residents}. Technologies include videoconferencing, the internet, store-and-forward imaging, streaming media, and landline and wireless communications.

Policy Statement

<CLIENT> authorizes the use of electronic information and audio or video telecommunications to provide health services for {patients/residents} without an in-person visit under the following criteria:

- Telehealth services must adhere to all Health Insurance Portability and Accountability Act (HIPAA) regulations including providing the Notice of Privacy Practices (NPP) as soon as practicable and conform to applicable local, state, and federal regulations.
- The health care provider must be designated as such by HHS and credentialed and licensed to provide health care services at the location of the {patient/resident}, except during public health emergencies or otherwise deemed acceptable by HHS/CMS/State laws.
- If a written consent is needed by <CLIENT> (or electronically captured) from the {patient/resident} to receive health care services, it shall be obtained via approved telehealth technologies.

- All existing regulations regarding {patient/resident} access to medical/clinical information and copies of such information, apply.
- In emergency situations, including public health emergencies, <CLIENT> may modify or waive provisions of this policy or procedures, in accordance with specific HHS waivers.
- <CLIENT> will follow all state and local guidelines for Telehealth in addition to federal regulations and guidance.
- Services via telehealth, remote patient monitoring, and virtual check-in can be provided to new and established patients.

Procedures

1. Telehealth should be used for the benefit of our {patients/residents} such as when travel is prohibitive, there is an imminent health risk justifying immediate medical services, or to provide health care services remotely rather than an in-person visit.
2. <CLIENT> will create procedures related to the billing and reimbursement of services provided for our {patients/residents} in compliance with state and federal laws as well as in accordance with third party payer's requirements.
3. A Business Associate Agreement (BAA) must be signed by any vendor for telehealth technologies to ensure that they meet the HIPAA privacy and security and breach notification standards. Such business associates may include:
    a. Telehealth hardware vendors
    b. Telehealth software vendors
    c. Medical device vendors
    d. Non-HIPAA covered entities
    e. Providers/Clinics where {patients/residents} may utilize their internet services for telehealth
4. The provider must advise the patient about the use of telehealth, potential risks, consequences, and benefits of telehealth technologies.
5. Providers must document all telehealth services as required by CMS and other payers in the {patient/resident}'s medical record.
6. Providers must use secure, HIPAA-compliant telecommunications technologies that use real-time audio and/or video communications with the {resident/patient}.
7. Telehealth records should be kept in the same manner as other health records by the provider, whether that is provided by an electronic health records vendor or other BA.

Security

1. Audio and Video conferencing platforms used for telehealth services must have the appropriate tools to authenticate individual users and secure transmission (such as end-to-end encryption).
2. The platforms must meet the privacy and security requirements of, and be compliant with, the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
3. The use of public-facing video communication applications is NEVER allowed, such as Facebook Live, Twitch, TikTok, and other similar applications.

4. Best practices should be used to mitigate privacy and security risks to the provider's organization and the {patient/resident}'s health information[1]:
    a. Use HIPAA-compliant messaging, voice and file transfer, and information storage;
    b. Provide effective and compliant storage in secure data centers that regularly conduct risk assessments with policies in place for reviewing controls;
    c. Integrate with existing communication systems, such as email, SMS, applications and pagers, as well as mobile phones and tablets;
    d. Securely distribute and access sensitive information from a mobile device, transmit media over industry-standard 256-bit SSL encrypted connections, and prevent access by unauthorized users or non-compliant devices;
    e. Leverage unique user identities, including usernames and passwords, and authenticated and role-based access at both the physical and IT level;
    f. Provide clear auditing ability for monitoring data integrity and access issues.

Enforcement & Exception Handling

Failure to comply with this policy, associated procedures and guidelines may result in disciplinary actions up to and including termination of employment or termination of contracts. Legal actions also may be taken for violations of applicable regulations and laws.

Request for exceptions to this policy must be submitted in writing. Prior to official approval of any exception, this policy must continue to be observed.

Definitions

Information System - Means any combination of information technology and people's activities that support operational, management and decision-making processes. A system normally includes hardware, software, information, data, applications, communications, and people.

Workforce Member - Means employees and other persons whose conduct, in the performance of work, are under the direct control of the organization, whether or not they are paid by the organization. This includes full and part time employees, contractors, affiliates, associates, students, and volunteers.

Distribution

This policy should be distributed to applicable Workforce Members. Recipients of this policy must acknowledge their receipt and understanding of this policy by referring any questions or problems with the policy within ten days of the issue date to the HIPAA Security Officer. If no questions or problems are stated, it will be assumed that the policy has been read and understood.

[1] *Source: AHIMA Telehealth Toolkit*

Applicable Regulations

HIPAA Security Rule	45 CFR Part 160 and Subparts A and C of Part 164
Contingency Operations	HIPAA §164.310(a)(2)(i)
Workstation Use	HIPAA §164.310 (b)

Revision History

Date:	Reviewed/Revised by:	New Changes	No Change √	Revision(s): State reason for revision	INITIALS