

Model Policy Kit

For FRHA Members

From the FRHA Summer Educational Series Event: Optimizing Telehealth and Work-From-Home Governance during COVID-19

**Prepared By:**

**Eagle Consulting Partners, Inc.**

6779 Memphis Ave. #7 | Cleveland, Ohio 44144

216.503.0333 | [www.eagleconsultingpartners.com](http://www.eagleconsultingpartners.com)

© 2020 Eagle Consulting Partners, Inc. All rights reserved. Healthcare provider is granted perpetual license to use and modify these policies for its own use. Redistribution other than to members of the Florida Rural Health Association is prohibited.

Contents

[Welcome 2](#_Toc49328596)

[Instructions for Adoption 2](#_Toc49328597)

[1000 Security Management Process 3](#_Toc49328598)

[1100 Encryption and Key Management 4](#_Toc49328599)

[1200 Computing Devices and Workstations – Organization-owned and BYOD 6](#_Toc49328600)

[2000 Employee Work at Home 8](#_Toc49328601)

[2100 Videoconferencing 10](#_Toc49328602)

[3000 Telehealth 11](#_Toc49328603)

[Additional Support and Resources 13](#_Toc49328604)

[About Eagle Consulting Partners 13](#_Toc49328605)

Welcome

Welcome to this Model Policy Kit prepared especially for Florida Rural Health Association members. Eagle and our partners at [ComplyALIGN](https://www.complyalign.com) were privileged to present “**Optimizing Telehealth and Work-From-Home Governance During COVID-19**” during the 2020 FRHA Summer Education Series.

This kit includes model policies your organization can implement for your own telehealth and work-from-home needs. It includes policies for:

* 1000 Security Management Process
* 1100 Encryption and Key Management
* 1200 Computing Devices and Workstations – Organization-owned and BYOD
* 2000 Employee Work at Home
* 2100 Videoconferencing
* 3000 Telehealth

These policies are drawn from Eagle’s comprehensive [*HIPAA Privacy and Security Policy Templates*](https://eagleconsultingpartners.com/hipaa-policy-templates-store/). All policies have been updated for compliance with the requirements of the HITECH Act of 2009, the Breach Notification Rule, and the HIPAA Omnibus Rule published January 25, 2013.

Instructions for Adoption

These draft policies must be customized based on the unique circumstances of the organization. For convenience, a global replace may be made to substitute the formal organization name for the character string “[HEALTHCARE PROVIDER]”. After appropriate customization, these draft policies may then be approved by management and integrated into relevant sections of the organization’s policy manual.

# 1000 Security Management Process

**POLICY**

The HIPAA Security Officer will orchestrate [HEALTHCARE PROVIDER]’s security management process.

**PURPOSE**

To ensure ongoing, effective management of [HEALTHCARE PROVIDER]’s computer security resulting in confidentiality, integrity and availability of electronic Protected Health Information.

**AUDIENCE**

CEO

HIPAA Security Officer

**REFERENCE**

[45 CFR 164.308](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=8a33ed5bd1a661000872c4d1799e61e2&r=PART&n=45y1.0.1.3.78#se45.1.164_1308)(a)(1) Security management process

**PROCEDURES**

1. The HIPAA Security Officer will orchestrate the security management process, with the support of any *Security and Compliance Team* appointed by the organization’s executive leadership. This will include:
   1. **Computer Security Risk Assessment**. A risk assessment will be maintained. The Risk Assessment is an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by [HEALTHCARE PROVIDER]. The Computer Security Risk Assessment will be handled as follows:
      1. [HEALTHCARE PROVIDER] will use the risk assessment methodology detailed in [NIST SP 800-30 Revision 1](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf) or the [FAIR](https://www.fairinstitute.org/what-is-fair) method.
      2. The risk assessment will guide the policy development and risk management process. Executive management will review the results of the risk analysis and maintain documentation of that review.
      3. The results of this assessment shall be documented and maintained for 6 years
      4. The Risk Assessment shall be updated on a periodic basis, as appropriate based on technical and environmental variables, product enhancements, infrastructure, or other technological changes.
   2. **Risk Management**. [HEALTHCARE PROVIDER] shall manage the risks identified in the risk analysis:
      1. [HEALTHCARE PROVIDER]’s Executive Management shall articulate its risk tolerance.
      2. Based on risk tolerance, and in consideration of probabilities and associated risk impacts, identified risks must be avoided, reduced, transferred (through contract or insurance) or accepted. These decisions shall be made by Executive Management or their designee.

Risk management decisions, corrective actions taken, project status and other related information shall be documented in a risk register. Documentation shall be maintained for 6 years.

* 1. **HIPAA Security Officer Accountability**. The HIPAA Security Officer is accountable for the following:
     1. Evaluate any regulatory requirements including HIPAA Security regulations, other applicable regulations, industry best practices, and environmental changes.
     2. Prepare recommendations for approval by [HEALTHCARE PROVIDER] management including implementation of new and updated policies, acquisition of technical security capabilities, or physical security measures.
     3. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level based on risk assessment and risk management decisions.
     4. Train employees regarding compliance. Compliance and other appropriate training shall be conducted for employees and contractors promptly after hiring and/or assignment to a HIPAA-regulated project.
     5. Monitor [HEALTHCARE PROVIDER]’s compliance with the information security policies and take corrective action as necessary to maintain compliance.

**REFERENCES**

[FAIR Institute](https://www.fairinstitute.org/)

Center for Internet Security at [www.cisecurity.org](https://www.cisecurity.org/)

# 1100 Encryption and Key Management

**POLICY**

Encryption with appropriate key management shall be used for data at rest and data in motion. Exceptions to approved procedures must be documented by the HIPAA Security Officer.

**PURPOSE**

To ensure that electronic Protected Health Information and other confidential information is protected from unauthorized access.

**AUDIENCE**

HIPAA Security Officer

**REFERENCE**

[45 CFR §164.312](https://www.ecfr.gov/cgi-bin/text-idx?SID=c9ad3bb1a7e5b54dd8dc9e52c2f74fee&mc=true&node=pt45.1.164&rgn=div5#se45.2.164_1312) (c), (d) and (e) Integrity, authentication and transmission security

[45 CFR §164.312(a)(2)(iv)](https://www.ecfr.gov/cgi-bin/text-idx?SID=c9ad3bb1a7e5b54dd8dc9e52c2f74fee&mc=true&node=pt45.1.164&rgn=div5#se45.2.164_1312) Encryption and Decryption [of data at rest]

**PROCEDURES**

1. **Encryption of Data at Rest**. Data at rest shall be encrypted using appropriate standards:
   1. **Servers and Cloud Environments**. Servers and cloud environments storing PHI at rest shall be encrypted using current standards:
      1. Cyphers shall be compliant with [ISO/IEC 19790:2012(E) Information technology – Security Techniques – Security requirements for cryptographic modules](https://www.iso.org/standard/52906.html).
   2. **Desktop, Mobile Devices and Portable Media**. When encryption of end-user devices is determined appropriate based on risk analysis, [HEALTHCARE PROVIDER] shall employ the framework detailed in [NIST Special Publication 800-111, *Guide to Storage Encryption technologies for End User Devices*](http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf). Specifically, the organization:
      1. should consider solutions that use existing system features (such as operating system features) and infrastructure
      2. should use centralized management for all deployments of storage encryption except for standalone deployments and very small-scale deployments
   3. **Keys and Key Management**.
      1. **Encryption Keys**. The HIPAA Security Officer shall ensure appropriate management for all encryption keys including those for cloud environments, servers, DBMS, backup media, desktop and mobile devices and other data assets.
      2. **Key Management**. Key management best practices shall be used for key assignment, backup, rotation, and destruction as detailed in [NIST SP 800-57 Part 1 Rev 4](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf), [NIST SP 800-57 Part 2](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf), and [NIST SP 800-57 Part 3](https://csrc.nist.gov/publications/detail/sp/800-57-part-3/rev-1/final).
      3. **Exceptions**. The HIPAA Security Officer may authorize exceptions to key management best practices, based on risk assessment. Any exceptions shall be documented.
2. **External Data in Motion**. For any data transmitted via the internet, [HEALTHCARE PROVIDER] systems shall use a securely configured transmission protocol that provides both encryption and message integrity.
   1. Acceptable transmission protocols include:
      1. Web Access: TLS 1.2 (HTTPS)
      2. File Transfer: FTPS, SFTP, SCP, WebDAV over HTTPS
      3. Remote Shell: SSH2 terminal
      4. Remote Desktop: radmin
   2. Secure configuration. Protocols shall be configured appropriately.
      1. Any encryption algorithms used must be compliant with [ISO/IEC 19790:2012(E) Information technology – Security Techniques – Security requirements for cryptographic modules](https://www.iso.org/standard/52906.html).
      2. The Secretary of HHS’s guidance (which provides a safe harbor) is may be used. The HHS guidance specifies the use of one of these standards:
         1. [NIST 800-77, *Guide to IPsec VPNs*](http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf)*,*
         2. [NIST 800-113, *Guide to SSL VPNs*](http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf)
   3. Exceptions. RDP may be used as a Remote Desktop Protocol only with the explicit approval of the HIPAA Security Officer who shall document the rationale for permitting the exception.
3. **Wireless Networks**. Wireless networks in [HEALTHCARE PROVIDER] facilities and/or employee home offices will be implemented with the following security options:
   1. The beacon shall be enabled
   2. The SSID should be changed from the default
   3. WPA2 should be enabled
   4. WPS should be disabled
   5. MAC filtering may be employed to allow access only to workstations owned by [HEALTHCARE PROVIDER] and authorized to use the network.
   6. These security options should be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.
   7. The administrator account shall be changed and protected with a strong password containing at least 12 characters, including 1 upper case, 1 lower case, and 1 digit, and shall conform with all other organizational requirements for passwords.

# 1200 Computing Devices and Workstations – Organization-owned and BYOD

**POLICY**

The organization maintains eligibility criteria to specify whether an employee is permitted to use

* Organization-owned desktop, laptop, smartphone and/ tablet, computing devices or
* personally-owned (BYOD) desktop, laptop, smartphone and/or tablet computing devices

to perform organization work and to access the organization’s IT resources. Employees using computing devices for organization business, whether a BYOD device or organization-provided, must follow all applicable requirements in this policy.

**PURPOSE**

To ensure the security of the organization and to establish standards for end-user computing devices including desktop workstations, laptops, tablets, and smartphones, including both organization-owned and personally-owned devices.

**DEFINITION**

**Bring Your Own Device (BYOD)** means the practice of an employee using a personally-owned computing device for organization purposes.

**AUDIENCE**

All Staff

**REFERENCE**

HIPAA Privacy and Security Rules, [45 CFR § 164](http://www.ecfr.gov/cgi-bin/text-idx?SID=c9ad3bb1a7e5b54dd8dc9e52c2f74fee&mc=true&node=pt45.1.164&rgn=div5)

[45 CFR § 164.312(b) Standard: Audit Controls](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=90921d878559759cce29b84663c0da01&mc=true&n=pt45.1.164&r=PART&ty=HTML" \l "se45.1.164_1312)

[45 CFR § 164.312(c)(1) Standard: Integrity](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=90921d878559759cce29b84663c0da01&mc=true&n=pt45.1.164&r=PART&ty=HTML#se45.1.164_1312)

[45 CFR § 164.312(d) Standard: Person or entity authentication](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=90921d878559759cce29b84663c0da01&mc=true&n=pt45.1.164&r=PART&ty=HTML#se45.1.164_1312)

[45 CFR § 164.312(e)(1) Standard: Transmission Security & (2) Implementation Specifications](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=90921d878559759cce29b84663c0da01&mc=true&n=pt45.1.164&r=PART&ty=HTML#se45.1.164_1312)

[45 CFR § 164.312(a)(2)(iv) Encryption and decryption](https://www.ecfr.gov/cgi-bin/text-idx?SID=c9ad3bb1a7e5b54dd8dc9e52c2f74fee&mc=true&node=pt45.1.164&rgn=div5" \l "se45.1.164_1312)

[45 CFR § 164.308(a)(5)(ii)(D) Password Management](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=90921d878559759cce29b84663c0da01&mc=true&n=pt45.1.164&r=PART&ty=HTML" \l "se45.1.164_1308)

[45 CFR § 164.308(a)(5)(ii)(B) Protection from Malicious Software](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=90921d878559759cce29b84663c0da01&mc=true&n=pt45.1.164&r=PART&ty=HTML#se45.1.164_1308)

**PROCEDURES**

1. **Eligibility.** The organization shall make a determination, on an individual basis, whether an employee is permitted and/or required to use either Organization-owned or employee-owned (BYOD) computing devices. Employees must follow the procedures in this policy that are applicable to the computing devices they use for organization business. Employees must sign either the Employee-Owned Device Agreement, or the Organization-owned Device Agreement, or both, as applicable.
2. **Portable Devices.** Employees using portable devices, whether BYOD or Organization-owned, must follow these safeguards:
   1. When traveling via automobile, portable computing devices may be left unattended only in a locked automobile trunk or other non-visible area of the automobile.
   2. When traveling via airplane, portable computing devices must be kept in carry-on luggage and kept in the possession of the employee during travel.
   3. When using public Wi-Fi networks to access organization or client systems, including email, encrypted connections such as VPN or TLS must be used.
   4. When working in a public setting, employees must maintain physical control of their devices at all times, be aware of their surroundings, and not allow unauthorized persons to view their screens. Access to production environments from public Wi-Fi is prohibited.
   5. Any device permitted by the HIPAA Officer to store PHI must be encrypted.
3. **EMPLOYEE-OWNED DEVICES (BYOD)**
   1. **Training**. The organization will provide training, as necessary, to employees on how to implement the security features required while using these devices.
   2. **Text** **Messaging**. Employees must not use standard text messaging to transmit PHI. Only the use of apps approved by the organization for transmitting PHI may be used to transmit PHI.
   3. **Reporting** **of Loss or Theft**. Loss of an employee-owned device authorized for organization use is a security incident and must be reported immediately.
   4. **Permission Granted for Remote Management, Lock/Wipe**. Employee grants the organization permission to enroll the any BYOD device in organization’s remote management system to enforce security configurations, to perform remote lock, remote wipe and/or geo-location of a device if deemed necessary by the organization.
   5. **Use of Device by Other People.** Employees using personal devices under this policy are responsible for controlling and/or managing the access and/or use of their device by other people including family members and friends. Employees will be held accountable for any actions performed by others who the employee permits to use the device.
   6. **Replacing a Device**. Prior to replacing/upgrading a device, employees must notify the organization and cooperate with the organization to ensure that all organization data and access privileges are removed prior to returning/selling/disposing of the device.
   7. **Sanctions for Violations**. Employees who violate any of the requirements of this policy will be subject to disciplinary action.
   8. **Discovery and other Legal Processes**. In case of legal action, personal devices used for the organization’s business are subject to e-discovery. Users are responsible for bringing or sending the mobile device to the organization office and giving the necessary device access codes when notified that the device is needed for e-discovery purposes.
   9. **Termination and/or Suspension from Employment.** Upon termination or suspension of employment, employee agrees to cooperate with the organization to ensure removal of all organization data and disabling of all access privileges granted to the device.
4. **ORGANIZATION-PROVIDED DEVICES**
   1. **Training**. The organization will provide training, as necessary, to employees on how to implement the security features required while using these devices.
   2. **Text Messaging**. Employees must not use standard text messaging to transmit PHI. Only the use of apps approved by the organization for transmitting PHI may be used to transmit PHI.
   3. **Reporting of Loss or Theft**. Loss of a computing device provided by the organization to an employee is a security incident and must be reported immediately.
   4. **Use for Organization Business Only.** Organization-owned devices must be used only for organization-related purposes, except that *minimum* personal use is permitted, such as checking weather or making a brief personal call.
   5. **Use of Device by Other People Not Permitted.** Employees using Organization-owned devices under this policy must not allow any unauthorized persons to use the device.
   6. **Organization-owned Devices May Not Be Sold, Transferred, Disposed of, Recycled or Damaged.** Employees must not sell, transfer, dispose of, recycle, or intentionally or recklessly damage Organization-owned devices.
   7. **Sanctions for Violations**. Employees who violate any of the requirements of this policy will be subject to disciplinary action.
   8. **Termination and/or Suspension from Employment.** Upon termination of employment or upon administrative leave, employee agrees to return the device to the organization.

# 2000 Employee Work at Home

**POLICY**

Employees who are eligible to work at home must follow these procedures to ensure data security. Baseline standards for home office must be met unless exceptions are made by the HIPAA Security Officer.

**PURPOSE**

To ensure that employees working from home do so in a secure, compliant, and effective manner.

**AUDIENCE**

All Staff

**REFERENCE**

HIPAA Privacy and Security Rules, [45 CFR § 164](http://www.ecfr.gov/cgi-bin/text-idx?SID=c9ad3bb1a7e5b54dd8dc9e52c2f74fee&mc=true&node=pt45.1.164&rgn=div5)

[45 CFR § 164.308(a)(5)(ii)(B) Protection from Malicious Software](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=90921d878559759cce29b84663c0da01&mc=true&n=pt45.1.164&r=PART&ty=HTML#se45.1.164_1308)

[45 CFR § 164.312(d) Standard: Person or entity authentication](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=90921d878559759cce29b84663c0da01&mc=true&n=pt45.1.164&r=PART&ty=HTML#se45.1.164_1312)

[45 CFR § 164.312(e)(1) Standard: Transmission Security & (2) Implementation specifications](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=90921d878559759cce29b84663c0da01&mc=true&n=pt45.1.164&r=PART&ty=HTML#se45.1.164_1312)

[45 CFR 164.312](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=8a33ed5bd1a661000872c4d1799e61e2&r=PART&n=45y1.0.1.3.78#se45.1.164_1312)(a)(2)(iv) Encryption and decryption

ISO 27002 11.7 Mobile computing and teleworking

**PROCEDURES**

1. **Eligibility for Work at Home**. Department leadership shall establish their policies regarding eligibility and/or requirement for mandatory work from home.
2. **Expectations**. Employees working from home are expected to be productive, to be available during normal business hours for organizational business and conferences, and to comply with all organizational policies and procedures regarding confidentiality and computer security.
3. **Stipend / Support**. The organization may offer a stipend to organizations who are mandated to work from home, to include support for internet expenses and other costs of maintaining a home office.
4. **Working from Home.** The HIPAA Security Officer shall review and approve home office arrangements by employees.
5. **Baseline Work from Home Security Standards**. Departments shall establish baseline standards for employee home environments. Unless an exception is granted, employees working from home must follow the Baseline Security Standards. Department leaders may consider the following standards based on the nature of the employee’s work:
   1. The home is equipped with physical security *appropriate for the neighborhood*, including, for example, deadbolt locks, home security system for high crime neighborhoods, and/or video monitoring.
   2. Exterior doors are kept locked when all occupants are away
   3. A dedicated room or section of the home is used exclusively for work. Preferably, this is a room with a lockable door.
   4. Access to the work area by other household members is restricted.
   5. Other household members are prohibited from using computing devices used for work (see [Policy 1060 Computing Devices and Workstations – Organization-owned and BYOD](#_1060_Computing_Devices))
   6. The home network is appropriately secured
      1. Vendor-supported Routers. The home office uses only routers which are actively supported by vendors.
      2. Router Configuration. The router must not use default administrator credentials, must use a strong password, remote management is disabled, and WPA2 encryption is enabled.
      3. Router firmware must be patched on a timely basis after a vendor-security update is published.
   7. The office is equipped with a shredder for destruction of any confidential paper documents.
   8. A clean-desk practice is followed so that any confidential materials are put away when not in use
   9. The organization reserves the right to require additional safeguards based on individual review
6. **Risk Assessment / Exceptions to the Baseline Standards**. The HIPAA Security Officer may perform an individual review for an employee/independent contractor’s work-from-home environment. This risk assessment shall consider:
   1. A review/risk assessment is conducted prior to authorizing exceptions to the Baseline Standards:
      1. The threat from outsiders / intruders in the neighborhood
      2. The threat of access by family and visitors to the remote working equipment
      3. The threat posed by other computing devices/individuals on the home network
      4. The physical layout of the home
      5. Other appropriate factors
   2. Based on this risk assessment, the HIPAA Security Officer may approve exceptions to the Baseline Standards.

# 2100 Videoconferencing

**POLICY**

Employees will use only videoconferencing platforms approved by the organization and shall conform to best practices when using those platforms.

**PURPOSE**

To ensure that only properly vetted and approved technologies are used by employees of the organization, and that their use of videoconferencing technologies are done in productive, respectful and compliant manner.

**AUDIENCE**

All Staff

**REFERENCE**

HIPAA Privacy and Security Rules, [45 CFR § 164](http://www.ecfr.gov/cgi-bin/text-idx?SID=c9ad3bb1a7e5b54dd8dc9e52c2f74fee&mc=true&node=pt45.1.164&rgn=div5)

[45 CFR § 164.312(e)(1) Standard: Transmission Security & (2) Implementation specifications](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=90921d878559759cce29b84663c0da01&mc=true&n=pt45.1.164&r=PART&ty=HTML#se45.1.164_1312)

[45 CFR 164.312](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=8a33ed5bd1a661000872c4d1799e61e2&r=PART&n=45y1.0.1.3.78#se45.1.164_1312)(a)(2)(iv) Encryption and decryption

ISO 27002 11.7 Mobile computing and teleworking

**PROCEDURES**

1. **Approved Vendors**. The Information Technology department shall approve and contract vendors. Vendors shall be vetted for privacy, security and HIPAA compliance with appropriate contracting.
2. **Employee Use**. Employees may use only approved vendors when initiating teleconferences and/or clinical encounters. Employees are permitted to participate in teleconferences initiated by 3rd parties, using the 3rd party’s technology.
3. **Etiquette for business and administrative videoconferences**. Employees should use proper etiquette during videoconferences:
   1. Obtain appropriate training regarding the use of the organization’s teleconferencing platform to know how to use key features including muting, enabling video, and ensuring proper functioning of ancillary equipment such as headsets and external speakers, so that technical malfunctions will not disrupt the call
   2. Be on time for meetings; introduce yourself when joining with people you don’t know
   3. Video cameras should be used for small meetings; for large meetings video may be turned off.
   4. Adjust lighting as necessary so that you can be seen clearly. Avoid windows in the background.
   5. Employees should place themselves on mute when not talking
   6. Appropriate etiquette should be followed including not eating, saying good-bye when leaving
   7. Ensure that all participants are notified in advance of recording
4. **Privacy / Security**. Ensure that appropriate privacy and security standards are used, including but not limited to:
   1. Ensure that a meeting password is used to limit access to those invited to the meeting
   2. Comply with HIPAA minimum necessary provision to limit the use of PHI to what is necessary
   3. Use any recording capability with care and ensure that appropriate security is enabled to limit access to those with a need to view the video.
   4. Ensure that an appropriate retention schedule is used for any video recordings.

# 3000 Telehealth

POLICY

The organization will operate telehealth programs to achieve appropriate clinical quality, patient satisfaction while complying with all legal, reimbursement and accreditation requirements.

PURPOSE

To ensure an effective and compliant telehealth program.

**AUDIENCE**

All Staff

**REFERENCE**

[State of Florida Department of Health Emergency Order No. 20-002](https://floridahealthcovid19.gov/wp-content/uploads/2020/03/filed-eo-doh-no.-20-002-medical-professionals-03.16.2020.pdf)

[State of Florida Telehealth Law, Chapter 2019-137](http://laws.flrules.org/2019/137)

[Ryan Haight Law](https://www.govinfo.gov/app/details/USCODE-2010-title21/USCODE-2010-title21-chap13-subchapI-partC-sec829)

JC Standard HRM.01.02.01 Comprehensive Accreditation Manual for Behavioral Health (Credentialing)

JC Standard HRM.01.01.03 EP2 Comprehensive Accreditation Manual for Behavioral Health (Scope of Practice)

JC Standard LD.04.01.01 EP2 Comprehensive Accreditation manual for Behavioral Health (Compliance)

JC Standard EM.02.02.13 Hospital and Critical Access Hospital Accreditation Manual (Emergency Management)

JC Standard EM.02.02.13 Ambulatory Health Care Accreditation Manual (Emergency Management)

HIPAA Privacy and Security Rules, [45 CFR § 164](http://www.ecfr.gov/cgi-bin/text-idx?SID=c9ad3bb1a7e5b54dd8dc9e52c2f74fee&mc=true&node=pt45.1.164&rgn=div5)

**DEFINITIONS**

**Telehealth**, per Florida statute, means the use of synchronous or asynchronous telecommunications technology by a telehealth provider to provide health care services, including, but not limited to, assessment, diagnosis, consultation, treatment, and monitoring of a patient; transfer of medical data; patient and professional health-related education; public health services; and health administration. The term does not include audio-only telephone calls, e-mail messages, or facsimile transmissions

**Telehealth provider** means any individual who provides health care and related services using telehealth and who is licensed under one of the chapters referenced in Section 456.47 of the Florida Statutes, paragraph (1)(b).

**PROCEDURES**

1. **Licensure.** All telehealth providers utilized by the organization shall comply with state licensure requirements:
   1. Patients in Florida. Telehealth providers treating patients in Florida must be licensed in Florida.
   2. Patients out of State. Telehealth providers treating patients in other states must be licensed in the state where the patient is located at the time of service.
2. **Credentialing and Registration.** All telehealth providers shall be appropriately credentialed per the organization’s credentialing policy [INSERT REFERENCE]. [Note: To streamline credentialing for the telehealth program, ensure that your credentialing policy provides for Credentialing by Proxy, that Medical Staff By-Laws include provision for credentialing by proxy, and that other legal and accreditation provisions are met.]
3. **Privacy and Security**. All HIPAA Privacy and Security standards apply to the telehealth practice. The HIPAA Security Officer or designee shall approve any telehealth platforms, which shall be evaluated based on the organization’s contracting and vendor management programs [INSERT REFERENCE]. Any audio or video recordings shall be maintained only when necessary based on clinical and risk management requirements, and that appropriate access controls and retention schedule is implemented.
4. **Practice Standards.** All telehealth providers shall conform to the practice standards relating to their scope of practice. Standards for telehealth services shall be the same as for in-person services.
5. **Prescribing of Controlled Substances.** Telehealth providers shall comply with federal and state regulations regarding prescription of controlled substances via telehealth.
6. **Accreditation.** The telehealth program shall comply with all applicable accreditation standards.
7. **Reimbursement.** The telehealth program shall comply with applicable requirements for third-party reimbursement, including appropriate credentialing, consent, licensure and other requirements.
8. **Informed Consent.** Prior to delivery of telehealth services, patients and/or their legal representatives shall sign informed consent regarding the risks and benefits of receiving services via telehealth. Consent may be signed electronically.
9. **Verification of Patient Identity and Location**. At the beginning of a clinical encounter via telehealth, the identity and location of the patient must be verified and shall be documented.
10. **Documentation.** All patient encounters shall be documented using the same documentation standards for in-person care, with the following additions:
    1. Where applicable, the documentation must be maintained both at the originating site and a the location of the provider
    2. Names and credentials of all clinical staff involved with the encounter, even when off-camera, shall be documented
    3. The fact that the encounter was conducted via telehealth modality must be documented.
11. **Quality Assurance**. Clinical managers shall ensure appropriate quality management for telehealth services, consistent with quality management policy [INSERT REFERENCE].
12. **Additional Procedures**. Additional clinical and administrative procedures shall be created as appropriate to address scheduling, patient technical support, clinician training, and specialty-specific and/or condition-specific protocols.

Additional Support and Resources

Questions About the Model Policy Kit

For specific questions about these sample policies, please contact Gary Pritts of Eagle Consulting Partners at 216-503-0333 or [info@eagleconsultingpartners.com](mailto:info@eagleconsultingpartners.com).

Comprehensive HIPAA Policies and Procedures

Both small and large organizations can benefit from Eagle’s policy customization services to develop and implement comprehensive HIPAA Privacy and Security policies for your organization. The HIPAA regulations require policies and procedures that are appropriate to the business and workflow of the organization, which necessitates vastly different policies depending on the type of organization.

We start with our library of comprehensive HIPAA Privacy and Security Policies specifically tailored for different types of entities. Then, working closely with you, we tailor the policies to your organization and integrate these policies with your existing policies and procedures manual. If desired, we can also facilitate management presentation and review.

More information is available at <https://eagleconsultingpartners.com/hipaa-policy-procedures-development/>.

Alternately, many of our comprehensive HIPAA Privacy and Security Policy templates can be obtained through our [Online Store](https://eagleconsultingpartners.com/hipaa-policy-templates-store/) for organizations that prefer to perform their own customization.

Over the last decade, Eagle has worked with and developed customized policy templates for a wide variety of HIPAA-covered entities, including physician practices, hospitals, TPAs, behavioral health organizations, public health departments, medical billing companies, IT and cloud computing companies, group homes for those with developmental disabilities, and more.

Cloud-based Policy Management Solution

ComplyALIGN provides a cloud-based policy management solution well-suited to the demands of a rapidly changing health care environment during COVID-19 and beyond. All FRHA members will receive a 20% discount using code “FRHA2020.” Visit [www.complyalign.com](http://www.complyalign.com) for more information.

About Eagle Consulting Partners

Eagle Consulting Partners helps healthcare-related organizations solve their cybersecurity, compliance, and IT risk management concerns so that they can achieve better quality, revenue, and care. We specialize in:

* Policy and Procedure Development
* Security Risk Assessments
* Disaster Recovery Planning
* Security Awareness Training
* Technical Vulnerability Assessment
* Regulatory Compliance Support

We have over 20 years of experience providing compliance and IT risk management services to many types of organizations, including hospitals, physicians, insurance plans, group homes for those with developmental disabilities, behavioral health agencies, home health agencies, and a variety of HIPAA Business Associates who provide services to healthcare organizations.

**We’d love to hear from you! Call us at 216-503-0333 or visit** [**www.eagleconsultingpartners.com**](http://www.eagleconsultingpartners.com)**.**