RioOne Health Network

Policy and Procedure Manual

Prepared by: Charles C. Stewart

RioOne Health Network

Approved by RioONE Board of Directors on February 28, 2013

DM-3	Direct Addresses	1	Draft	98
DM-4	Trusted HISPs	1	Draft	99
DM-5	Agreements with RioOne Health Direct Users	1	Draft	100
DM-6	Use and Disclosure of PHI in RioOne Direct Messaging	1	Draft	101
Policy Identification	**Title**	**Version**	**Effective Date**	
DM-7	Data Backup Plan and Disaster Recovery Plan	1	Draft	102
DM-8	RioOne Direct Messaging User Enrollment	1	Draft	103
DM-9	Direct User Suspension and Termination	1	Draft	105
DM-10	Direct Messaging Training	1	Draft	107
DM-11	Direct Messaging Service Log-In and Log-Off	1	Draft	108
DM-12	RioOne Direct Messaging Password Management	1	Draft	110
DM-13	Deletion of RioOne Health Direct Messages	1	Draft	111
DM-14	RioOne Direct Messaging Encryption and Decryption	1	Draft	112
	Appendix A Documents			
App-A	IT Security and Risk Management Plan	1	Draft	
App-A	Participant Agreement	1	Draft	
App-A	Subscriber Agreement (Cerner)	1		
App-A	Patient Demographics	1		

App-A	Sanitation PHI Disposal Tables (HS-18)	1		
	Appendix B Forms			
App-B	Direct Messaging/Project Form	1		
App-B	Patient Authorization Form (HP-1)	1		
	Appendix B Forms			
App-B	Suspend and Accounting Form (HP-6)	1		
App-B	Sanction Breach Form (HP-10)	1		
App-B	Confidentiality Agreement Form (HS-4)	1		
App-B	Certificate of PHI Disposal (HS-18)	1		
App-B	Breach Notification Assessment Form (HS-25)	1		
App-B	Individual Breach Notification Letter (HS-25)			
App-B	Audit Request Form (DM-7)			
	Appendix C "Participant Membership List/ Provider Directory"			
App-C	Membership Spreadsheet			

	Appendix D **“Revision Tracking Sheet”**			
App-D	Tracking Spreadsheet			

Introduction to the Policy and Procedure Manual

RioOne Health is the Health Information Exchange (HIE) for the Rio Grande Valley (South Texas). It provides a secure, confidential, electronic system to support the exchange of patient medical records among health care providers, in South Texas and beyond. RioOne Health will provide health care providers with two ways to exchange patient records: RioOne Health Information Exchange and RioOne Health Direct Messaging.

RioOne Health Information Exchange is a collection of standards, policies and message based services providing a secure method for RioOne Health Information Exchange Participants and their users to query and retrieve patient data across all RioOne Health Information Exchange Participants. RioOne Health Information Exchange is based on the Nationwide Health Information Network specifications and standards supported and maintained by the Office of the National Coordinator of Health Information Technology (ONC).

RioOne Health Direct Messaging allows providers to share health information electronically in a method similar to regular email but with the added security required for sensitive health information. RioOne Health Direct Messaging is a 'push' secure messaging system where information is sent from one registered provider directly to another registered provider who is known to the sender. RioOne Health Direct Messaging is based on the National Direct Project, which was launched in March of 2009, by the Office of the National Coordinator of Health Information Technology (ONC).

This Policy and Procedure Manual contains policies and procedures that implement the policy decisions which underlie RioOne Health. They will inform all Participants and Users of the "rules of the road" for the HIE and Direct Messaging, in addition to the trust agreements that each Participant and User signs.

Governing Body Policies and Procedures

The RioOne Health Governing Body is responsible for setting the overall strategic direction for RioOne Health as well as overseeing its development and implementation. Working with the State of Texas HIE Executive Director and the other strategic advisors, the RioOne Health Governing Body will guide the implementation of technical and policy components that are critical to a successful health information exchange.

The Governing Body Policies and Procedures describe the ways in which the RioOne Health Governing Body will operate to maximize its effectiveness and transparency. They include basic organizational policies and procedures as well as those that describe how the Governing Body meetings will be operated in compliance with all State of Texas requirements.

HIPAA Privacy and Security

Overview

RioOne Health is in the business of helping providers securely exchange health information. Therefore, RioOne Health has written Privacy and Security Policies and Procedures to affirm its commitment to comply with the applicable provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The net effect of these laws is that RioOne Health is required to comply with certain provisions of the HIPAA Privacy and Security Regulations. The Policies and Procedures included in this Manual provide the framework through which RioOne Health will comply.

HIPAA Privacy Policies and Procedures

The HIPAA Privacy Regulations provide rules regarding the use and disclosure of PHI (Personal Health Information), as well as specific rules regarding an individual's rights to access PHI. As a Business Associate, RioOne Health is required to follow all requirements of the HIPAA Privacy Regulations. RioOne Health's Privacy Officer will oversee its compliance with the HIPAA Privacy Regulations and its efforts to protect the privacy of all PHI that is exchanged through the Network. RioOne Health will consistently monitor, and periodically audit, its Privacy practices to ensure compliance with the Privacy Policies and Procedures.

HIPAA Security Policies and Procedures

Under the HIPAA Security Regulations, Covered Entities and Business Associates are required to implement administrative, physical, and technical safeguards that ensure the confidentiality, integrity, and availability of ePHI. These safeguards are designed to:

1. Ensure the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains, or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted by the HIPAA Privacy Regulations; and,
4. Ensure compliance with the HIPAA Security Regulations by its workforce.

The Security Policies and Procedures in this Manual address RioOne Health's obligations under the HIPAA Security Regulations. In designing these policies and procedures, RioOne Health has considered:

1. RioOne Health's size, complexity, and capabilities;
2. RioOne Health technical infrastructure, hardware, and software security capabilities;
3. The costs of security measures; and
4. The probability and criticality of potential risks to ePHI.

RioOne Health's Security Officer will oversee RioOne Health's initiatives to create and maintain appropriate and reasonable policies, procedures, and controls to protect the security of ePHI exchanged through the Network.

Network Operations Policies and Procedures

The RioOne Health Network consists of two components – RioOne Health Direct Messaging and RioOne Health Information Exchange. While these components are separate and distinct from each other, there are some operational similarities. The Network Operations Policies and Procedures include general policies and procedures that describe how the overall RioOne Health Network will be operated.

General HIPAA
Policies and Procedures

RioOne Health	General HIPAA Policies	Policy ID: H-1
Title: **Defined Terms**	Version: 1	Effective Date: **Draft**

For the purposes of the RioOne Health General HIPAA Policies, Privacy Policies and Security Policies, the following terms shall have the meaning ascribed to them below.

Addressable: Addressable refers to implementation specifications contained within certain HIPAA Regulations which RioOne Health is not required to implement. RioOne Health must perform an assessment to determine whether the addressable implementation specification is a reasonable and appropriate safeguard for implementation in its efforts to protect unauthorized use, disclosure, and access of PHI or ePHI. If it is not reasonable and appropriate, RioOne Health must document the reasons supporting this conclusion.

Administrative Safeguards: Administrative Safeguards are actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of Users in relation to the protection of ePHI.

Breach: The unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Business Associate: A Business Associate is a person or entity who, on behalf of a Covered Entity, performs, or assists in the performance of, a function or activity involving the use or disclosure of individually identifiable health information, including, but not limited to, facilitation of the exchange of health information; claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; or practice management.

RioOne Health Direct Messaging: A service provided by RioOne Health to RioOne Health Direct Users that allows the User to send and receive secure messages utilizing the Direct Project specifications and an Internet-based service provided by RioOne Health.

RioOne Health Direct Messaging Service: A user interface provided by RioOne Health to RioOne Health Direct Users that allows such Users to access and use RioOne Health Direct Messaging.

RioOne Health Direct User: An individual clinician who is regulated by the State of Texas Department of Health Professions who has successfully enrolled in RioOne Health Direct Messaging.

RioOne Health Direct User Information: RioOne Health Direct User Information means demographic information about RioOne Health Direct Users provided to RioOne Health during the RioOne Health Direct Messaging enrollment process or in accordance with the Direct Messaging End User License Agreement.

RioOne Health Information Exchange: An Internet-based service provided by RioOne Health to RioOne Health Information Exchange Participants that allows the Participant and individual users authorized by the Participant to query and retrieve clinical data from other RioOne Health Information Exchange Participants, if permitted by applicable law and the RioOne Health Policies and Procedures.

RioOne Health Information Exchange Participant: An organization that has met the eligibility criteria for participation in RioOne Health Information Exchange and has been accepted as a RioOne Health Information Exchange Participant by the RioOne Health Governing Body.

Contingency Event: A Contingency Event is an unplanned for event, such as an emergency or disaster, which may require the activation of RioOne Health's IT Security and Risk Management Plan (Contingency Plan, Data Back-Up Plan, Disaster Recovery Plan, or Emergency Operations Plan).

Covered Entity: A Covered Entity is (i) a health plan, (ii) a health care clearinghouse, or (iii) a health care provider who transmits any health information in any form, including in electronic form. For purposes of this HIPAA Privacy and Security Policy and Procedures Manual, Covered Entity means RioOne Health Information Exchange Participants or RioOne Health Direct Users who utilize the Network, including health care providers, medical practices, and laboratories.

Electronic Protected Health Information or ePHI: Electronic PHI means PHI which is either transmitted by electronic media or maintained in electronic media.

HIPAA Regulations: HIPAA Regulations means the Health Insurance Portability and Accountability Act of 1996 and the rules and regulations promulgated thereunder, and the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. §§ 17921-17954) and the rules or regulations promulgated thereunder.

Network: The Internet-based network established by RioOne Health that allows RioOne Health Information Exchange Participants and RioOne Health Direct Users to transact information with each other and others, as permitted by RioOne Health pursuant to the RioOne Health Information Exchange Participation Agreement, the Direct Messaging End User License Agreement or RioOne Health Policies and Procedures. The Network includes both RioOne Health Direct Messaging and the RioOne Health Information Exchange.

Physical Safeguards: Physical Safeguards are physical measures, policies, and procedures to protect the Network and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Privacy Officer: Privacy Officer means the individual named in the Assigned Privacy Responsibility Policy (HP-7).

Protected Health Information or PHI: PHI means health information that is individually identifiable.

Required: Required refers to implementation specifications contained within certain HIPAA regulations with which RioOne Health must comply.

Security Incident: Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations of the Network.

Security Officer: Security Officer means the individual named in the Assigned Security Responsibility Policy (HS-3).

Technical Safeguards: Technical Safeguards means the technology and the policy and procedures that RioOne Health has to protect ePHI and control access to it.

User: A person or entity with authorized access to the Network. Users include Workforce Members, RioOne Health Direct Users, employees and agents of RioOne Health Information Exchange Participants who are authorized to use the Network, and Vendors.

Vendor: Vendor means a vendor, consultant, contractor or other non-RioOne Health third party who may have access to the Network for any reason or purpose (other than those who may have incidental access) or who may have access to any RioOne Health facilities housing the information technology assets that support the Network or related infrastructure.

Workforce Member: All persons who are under the control of RioOne Health, including, but not limited to, employees, independent contractors, loaned personnel, interns, and temporary personnel and who have access to the Network or any PHI derived from the Network.

Workstation: Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

RioOne Health	General HIPAA Policies	Policy ID: H-2
Title: **Workforce Member Confidentiality and Compliance Statement**	Version: 1	Effective Date: **Draft**

Purpose Statement: All Workforce Members are required to certify in writing, by signing the Workforce Member Confidentiality and Compliance Statement provided below, that they have completed a mandatory training, and have read and understand and agree to follow the policies in the manual that has been provided, along with all applicable provisions of HIPAA and the HITECH Act. Also, as part of their compliance with these Policies and Procedures, Workforce Members must certify that they will protect the confidentiality of PHI, including ePHI, and that they will report any unauthorized disclosures of PHI or ePHI and other Security Incidents to the Privacy Officer or Security Officer, as specified in this manual.

Policy/Procedure:

1. All Workforce Members will sign the Workforce Member Confidentiality and Compliance Statement provided below prior to being given access to PHI, ePHI or the Network and annually thereafter.
2. The Privacy Officer will maintain a record on each Workforce Member that includes the original, signed Workforce Member Confidentiality and Compliance Statements.
3. The Privacy Officer will return a copy of the signed Workforce Member Confidentiality and Compliance Statement to the Workforce Member.
4. Any Workforce Member that refuses to sign the Workforce Member Confidentiality and Compliance Statement will be sanctioned in accordance with the Workforce Member Discipline Policy (H-3).

WORKFORCE MEMBER HIPAA CONFIDENTIALITY AND COMPLIANCE STATEMENT

I, _____, acknowledge that I have received, read, received training on, understand and agree to follow the RioOne Health HIPAA Privacy and Security Policies and Procedures that have been given to me for my review. Also, I acknowledge that during the course of performing my assigned duties at RioOne Health, I may have access to, use, or disclose Protected Health Information (PHI) or electronic PHI (ePHI). I agree to handle such information in a confidential manner at all times during and after my employment and commit to the following obligations:

1. I will use and disclose PHI, including ePHI, only in connection with and for the purpose of performing my assigned job functions.
2. I will request, obtain, or communicate PHI, including ePHI, only as necessary to perform my assigned job functions and will refrain from requesting, obtaining or communicating more PHI, including ePHI, than is necessary to accomplish such functions.

3. I will take reasonable care to properly secure PHI, including ePHI, on my Workstation and will take steps to ensure that others cannot view or access such information.
4. I will use and disclose PHI, including ePHI, solely in accordance with the applicable federal and state laws and regulations and all RioOne Health HIPAA Privacy and Security Policies and Procedures. I also agree, in a timely manner, to familiarize myself with any periodic updates or changes to these policies.
5. I will immediately report any unauthorized use or disclosure of PHI, including ePHI, that I become aware of to the appropriate RioOne Health Official.
6. I understand and agree that my failure to fulfill any of the obligations set forth in this Statement and any failure to comply with the RioOne Health's HIPAA Privacy and Security Policies and Procedures will result in my being subject to appropriate disciplinary action, up to and including, the termination of my employment.

_____	_____
Workforce Member's Signature	Privacy Officer's Signature
_____	_____
Date	Date
_____	_____
Workforce Member's Printed Name	Privacy Officer's Printed Name
_____	_____
Workforce Member's Job Function/ Department	Hire Date

Responsibility: Privacy Officer; Workforce Member

Regulatory Category: Privacy Regulations; Security Regulations

RioOne Health	Governing Body	Policy ID: H-3
Title: **Workforce Member Discipline**	Version: 1	Effective Date: **Draft**

Purpose Statement: RioOne Health will discipline Workforce Members, as necessary, for violations of its HIPAA Privacy and Security Policies and Procedures.

Policy/Procedure:

MINOR OCCURRENCES

If the Privacy or Security Officer determines that a Workforce Member's acts or omissions resulted in a relatively minor violation of these HIPAA Privacy and Security Policies and Procedures and no significant violation of any law or regulation, the respective Officer will determine whether or not further education, clarification, or other corrective actions are needed.

SIGNIFICANT VIOLATIONS

If the Privacy or Security Officer determines that a Workforce Member's acts or omissions resulted in a significant violation of these HIPAA Privacy and Security Policies and Procedures or a violation of any law or regulation, the respective Officer will report the findings to the RioOne Health Executive Director, and will recommend appropriate disciplinary action. The RioOne Health Executive Director will then determine the scope of any disciplinary steps to be taken.

DISCIPLINARY ACTION

1. Disciplinary action should be commensurate with the seriousness of the security or privacy violation. Discipline may take one or more forms, including, but not limited to:
    a. Oral counseling and admonishment
    b. Written reprimand
    c. Requiring the Workforce Member to attend training
    d. Reassignment
    e. Demotion and/or reduction in pay
    f. Suspension without pay
    g. Termination of employment
2. The Executive Director will consult with legal counsel at his discretion to determine what disciplinary action is appropriate.

Responsibility: Privacy Officer; Security Officer; Executive Director

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.308(a)(1)(ii)(C), Sanction Policy [Implementation Specification; Required]

RioOne Health	General HIPAA Policies	Policy ID: H-4
Title: **Breach and Security Incident Response Procedures**	Version: 1	Effective Date: **Draft**

HITECH Act Language:
"A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach."

"For purposes of this section, a breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred."

"Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved in the case of a notification required under subsection (b))."

HIPAA Security Rule Language: "Implement policies and procedures to address security incidents."

Purpose Statement: Despite taking all reasonable and appropriate steps to protect the confidentiality, integrity and availability of ePHI and the Network, RioOne Health may experience Security Incidents and/or Breaches. RioOne Health will promptly identify, report, track, and respond to Security Incidents and potential Breaches. Awareness of, response to, and creation of reports about Security Incidents and Breaches are integral parts of RioOne Health's efforts to comply with the HIPAA Regulations.

Policy/Procedure:

SECURITY INCIDENTS

1. A "Security Incident" is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations through the Network.
2. The following incidents are examples of potential Security Incidents. This list is not exclusive. The Security Officer will determine when a Security Incident has or is likely to have occurred.

a. Stolen or otherwise inappropriately obtained passwords that are used to access the Network;
b. Corrupted backup tapes that do not allow restoration of ePHI through the Network;
c. Virus attacks that interfere with the operations of the Network;
d. Physical break-ins to RioOne Health's facilities which may lead to the theft of electronic media containing ePHI;
e. RioOne Health's failure to terminate the account of a former RioOne Health Direct User that is then used by an unauthorized individual to access the Network; and/or
f. Allowing electronic media containing ePHI, such as a computer hard drive or laptop, to be accessed by a User who is not authorized to access such ePHI prior to removing the ePHI stored on the media.

BREACHES

1. A Breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
2. The HITECH Act Breach notification requirements only apply to PHI that is "unsecured." "Unsecured" PHI is that PHI which is not secured through a technology or methodology that the Department of Health and Human Services (HHS) has stated renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals.
3. According to guidance issued by HHS in August 2009 (the most recent guidance issued by HHS on this topic as of the creation date of this Policy), PHI is secured through encryption (for ePHI) or destruction (for PHI in all other formats).
4. RioOne Health will take all measures necessary to secure PHI in accordance with the Device and Media Controls (HS-18), Technical Access Controls (HS-19), and Transmission Security (HS-22) Policies included in this Manual.
5. In addition, the following occurrences are not Breaches:
    a. Any unintentional acquisition, access, or use of PHI by a Workforce Member or individual acting under the authority of RioOne Health if:
        i. Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such Workforce Member or individual, respectively, with RioOne Health; and
        ii. Such information is not further acquired, accessed, used, or disclosed by any person.
    b. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by RioOne Health to another similarly situated individual at the same facility and any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

IDENTIFYING POTENTIAL BREACHES AND SECURITY INCIDENTS

1. RioOne Health will be responsible for monitoring and auditing activities. RioOne Health will, on a regular basis, review audit reports which provide a summary of all uses of the Network.
2. The following findings in the audit reports will signal a potential Breach or Security Incident:
   a. A single RioOne Health Direct User sending more than five messages through RioOne Health Direct Messaging between the hours of 12:00 am – 5:00 am
   b. Failed authentication attempts after five (5) unsuccessful attempts
   c. Activity originating from an I/P address outside of country

REPORTING POTENTIAL BREACHES AND SECURITY INCIDENTS

1. Any Workforce Member, including RioOne Health management, must report any potential Breach or Security Incident that he or she discovers, or any other potential threat to the confidentiality, integrity, or availability of ePHI exchanged through the Network, to the Privacy Officer immediately upon discovery of the potential Breach, Security Incident or threat.
2. Any RioOne Health Direct User, other than a Workforce Member, must immediately report any potential Breach or Security Incident that he or she discovers, or any other potential threat to the confidentiality, integrity, or availability of ePHI exchanged through the Network to the RioOne Health Systems Administrator. The Systems Administrator will then forward the notice to the RioOne Health Privacy Officer.
3. The individual providing notice of the potential Breach, Security Incident or other threat may provide such notice in any format, including in writing, electronically, or orally.
4. The Privacy Officer will document the report of a potential Breach or Security Incident or threat along with the date and time that he or she was notified of such event.
5. RioOne Health will not take any retaliatory measures against an individual who reports a potential Breach or Security Incident or threat. If the Breach or Security Incident was created by the neglect, or deliberate action, of a User, then RioOne Health may impose sanctions as set forth in other Policies (HP-10).
6. No RioOne Health Information Exchange Participant or User will prohibit or otherwise attempt to hinder or prevent another RioOne Health Information Exchange Participant or User from reporting a potential Breach, Security Incident or threat.

RESPONSE TO POTENTIAL BREACHES AND SECURITY INCIDENTS

1. Upon becoming aware of a potential or suspected Breach or Security Incident, the RioOne Health Privacy Officer will immediately activate the Incident Response Team. The Incident Response Team shall be composed of the RioOne Health Executive Director, the RioOne Health Privacy Officer, the RioOne Health Security Officer, the RioOne Health Technical Expert, RioOne Health Legal Counsel and the Chairperson of the Compliance Committee. The RioOne Health Executive Director will be the Incident Response Leader.
2. The Incident Response Team will promptly conduct an initial review of the facts surrounding the potential Breach or Security Incident to determine whether a Breach or

Security Incident occurred. The Incident Response Team will strive to make an initial determination within 48 hours of becoming aware of the potential Breach or Security Incident.

3. If the Incident Response Team determines that a Breach or Security Incident did not occur, the RioOne Health Privacy Officer will document this along with all of the information that supports such conclusion and no further investigations are required. The Privacy Officer will present a summary of the Committee's findings at the next meeting of the RioOne Health Governing Body.
4. If the Incident Response Team determines that a Breach or Security Incident did occur or is likely to have occurred, then the following steps will be followed:
    a. The Incident Response Team will determine the scope, magnitude and severity of the Breach or Security Incident; mechanisms for containing the Breach or Security Incident if it is on-going; mechanisms for mitigating the harmful effects of the Breach or Security Incident; and, ways to remediate the vulnerability that led to the Breach or Security Incident. The Incident Response Team will prepare these initial findings within 72 hours of becoming aware of the potential Breach or Security Incident and will update those findings as more information becomes available.
    b. The Incident Response Team will determine which RioOne Health Information Exchange Participants or RioOne Health Direct Users, if any, should be involved in the investigation and mitigation activities and involve such Participants and Users as the Committee deems appropriate.
    c. The Incident Response Team will officially notify all affected RioOne Health Information Exchange Participants or RioOne Health Direct Users of a Breach or Security Incident within ten (10) business days of becoming aware of such Breach or Security Incident. The notification will include the following information:
        i. The date of the Breach or Security Incident.
        ii. The identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such Breach or Security Incident, if it can be determined.
        iii. A description of the roles of the people involved in the Breach or Security Incident such as, but not limited to, Users, Workforce Members, Vendors or unauthorized persons.
        iv. The type of information that was Breached or involved in the Security Incident, if it can be determined.
        v. A brief description of the circumstances involved in the Breach or Security Incident.
    d. Legal counsel will determine whether RioOne Health is required to make

any additional notifications pursuant to applicable breach notification laws and discuss such notifications with the Incident Response Team and the affected RioOne Health Information Exchange Participants and RioOne Health Direct Users.

e. If RioOne Health has determined that a RioOne Health Direct User's noncompliant behavior caused a Breach or Security Incident, RioOne Health will determine the appropriate corrective action to pursue, including termination of the RioOne Health Direct User's authorization to use RioOne Health Direct Messaging. The RioOne Health Direct User must abide by whatever corrective action RioOne Health decides to pursue regarding the noncompliant behavior.

g. The Executive Director will notify the RioOne Health Governing Body Chair of the results of the Incident Response Team's findings. The Chair will provide guidance to the Executive Director regarding how to communicate the findings to the full Governing Body.

h. The Security Officer will retain all documentation regarding the Breach or Security Incident for six years.

OTHER MEASURES REGARDING BREACHES AND SECURITY INCIDENTS

1. RioOne Health will provide training and awareness materials to Users, as appropriate, regarding the process for promptly identifying, reporting, tracking, and responding to potential Breaches and Security Incidents in accordance with this Policy.
2. As deemed necessary by the Privacy Officer, RioOne Health will take disciplinary action, including termination if deemed necessary, in accordance with the Workforce Member Discipline Policy (H-3) against Workforce Members whose actions lead to or cause Breaches or Security Incidents.
3. No User who reports a suspected Breach or Security Incident that is caused by another User will face retaliation from RioOne Health.

Responsibility: Privacy Officer, Security Officer, Executive Director, RioOne Health Information Exchange Participant, User, Workforce Member

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(6)(i), Security Incident Procedures [Standard; Required]

- 45 C.F.R. §164.308(a)(6)(ii), Response and Reporting (of Security Incidents) [Implementation Specification; Required]

RioOne Health	General HIPAA Policies	Policy ID: H-5
Title: **Participant Agreement Policy**	Version: 1	Effective Date: **Draft**

PURPOSE:
To secure written Participation Agreements with each Participant of RioOne Health binding Participants to comply with applicable laws, requirements of THSA, and RioOne Health policies and procedures on use of the Exchange as outlined in this Policy.

POLICY: When using the Exchange, each Participant will:

1. Execute a Participation Agreement and attached Business Associate Agreement.
2. Comply with applicable federal and state laws and regulations, including, but not limited to those protecting the confidentiality and security of PHI and establishing individual privacy rights and use reasonable efforts to stay abreast of any changes or updates and interpretations of laws and regulations.
3. Be aware of the provisions of certain state laws, which are [or may be] more stringent than, and not preempted by, the HIPAA Privacy and Security Regulations.
4. Have the requisite, appropriate, and necessary internal policies for compliance with applicable state and federal privacy and security laws and RioOne Health's Participant Agreement, including, without limitation, a sanctions policy. Participant will enforce its policies and procedures by appropriately sanctioning any employee, volunteer, contractor, subcontractor or other person who accesses the Exchange on behalf of the Participant.
5. Have policies and procedures to promote the accuracy and relevance of the PHI it makes available through the Exchange.
6. Acknowledge and agree that the PHI transmitted to the Exchange, including but not limited to the Provider Directory, Master Patient Index, and Record Locator Service does not constitute a Designated Record Set as defined by HIPAA.
7. Will not exclusively rely on documents transmitted through the Exchange to make treatment decisions.
8. Ensure that patient authorization has been obtained prior to transmitting any PHI through the Exchange.
9. Update its Notice of Privacy Practices ("NPP") to describe its participation in the Exchange when an individual has authorized his/her PHI to be used or disclosed through the Exchange.
10. Designate individuals who may access the Exchange on behalf of Participant. Only Workforce members who have a legitimate and appropriate need to use the Exchange shall be granted access. No Workforce member will be provided with access to the Exchange without training. Participant will require that Workforce members:

A. Receive training regarding the confidentiality and security of PHI and the requirements set forth by HIPAA, HITECH, and state confidentiality laws;

B. Only access the Exchange for purposes of (1) treatment, (2) payment, and/or (3) necessary health care operations as allowed by law. Except for treatment, each Participant will access or enter into the Exchange only the minimum amount of PHI necessary for the purpose of the access or entry;

C. Hold any passwords, or other means for accessing the Exchange, in a confidential and secure manner and release them to no other individual; and

D. Comply with applicable RioOne Health Polices and those of the Participant. Workforce members must understand that failure to comply with such policies and procedures may constitute cause for disciplinary action, up to and including termination and the imposition of civil and criminal penalties against Participant.

11. Each Participant will provide RioOne Health with the name, telephone number, facsimile, and e-mail of its current Privacy Officer.

HIPAA Privacy
Policies and Procedures

RioOne Health	HIPAA Privacy	Policy ID: HP-1
Title: **Uses and Disclosures of PHI**	Version: 1	Effective Date: **Draft**

HIPAA Privacy Rule Language:

> **PERMITTED USES AND DISCLOSURES—§164.506**
> "Except with respect to uses or disclosures that require an authorization under §164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations…provided that such use or disclosure is consistent with other applicable requirements of this subpart."

USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION IS REQUIRED—§164.508

"Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization."

Purpose Statement: RioOne Health will only use or disclose PHI as permitted by its RioOne Health Information Exchange Participation Agreements and RioOne Health Direct Messaging End User License Agreements.

Policy/Procedure:

1. RioOne Health may only use or disclose PHI to fulfill its responsibilities under the RioOne Health Information Exchange Participation Agreement or the RioOne Health Direct Messaging End User License Agreement. This includes, but is not limited to, performing proper management and administrative functions.
2. RioOne Health's uses and disclosures of PHI in connection with RioOne Health Direct Messaging are more fully described in RioOne Health's Use and Disclosure of PHI in RioOne Health Direct Messaging Policy (DM-6).
3. All PHI will automatically be transmitted through the Exchange until the individual has signed an **"Opt-Out" form,** which deauthorizes, disallowing his or her PHI to be transmitted through the Exchange. The deauthorization must have language approved by RioOne Health Network.
4. The Exchange will use an **Opt-Out** process, and will not segment PHI. This means that all PHI about that individual will be available through the Exchange, including alcohol and substance abuse, HIV/Aids, mental health and psychotherapy notes, STDs, hepatitis and genetic testing.
5. Participants are responsible for complying with all state laws, THSA regulations, and HIPAA requirements governing deauthorization. Participants shall ensure that the deauthorization form incorporates all law and HIPAA requirements. Participants shall

indemnify the Exchange against any and all causes of action and damages based on use by Participant of a deauthorization "**Opt-Out" form** that fails to comply with state and federal law.

6. When a Participant obtains an individual's written or electronic deauthorization to transmit is/her PHI through the Exchange, the Participant will be keep such deauthorization on file at the Participant office or facility.
7. An individual may revoke an authorization/deauthorization at any time, provided the revocation is in writing. RioOne Health Network will stop transmitting information about that individual as soon as possible but at least within seventy-two (72) hours of receipt of written notice that an individual has revoked his/her authorization. RioOne Health Network will not be liable for use or disclosure of an individual's PHI after a revocation if:
   - RioOne Health Network is not made aware that an individual revoked his/her authorization; or HIPAA/HITECH Privacy Compliance Manual Page 10
   - RioOne Health Network, in good faith, based its actions upon a prior authorization, and has already acted in reliance on that authorization.

Responsibility: Privacy Officer; RioOne Health Direct User

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.506, Uses and Disclosures to Carry Out Treatment, Payment, or Health care Operations [Standard; Required]
- 45 C.F.R. §164.508, Uses and Disclosures for which an Authorization is Required [Standard; Required]

RioOne Health	HIPAA Privacy	Policy ID: HP-2
Title: **Minimum Necessary Standard**	Version: 1	Effective Date: **Draft**

HIPAA Privacy Rule Language: "A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

"For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

"For all other requests, a covered entity must: (A) develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and (B) review requests for disclosure on an individual basis in accordance with such criteria."

Purpose Statement: RioOne Health will use reasonable efforts to limit PHI or ePHI that it uses or discloses as part of its management and administration of the Network to the least amount necessary (the "minimum necessary") to accomplish the intended purpose of the disclosure. This policy encompasses PHI in any format, such as oral, electronic, or written.

Policy/Procedure:

RioOne Health will limit all uses and disclosures of or requests for PHI to the minimum necessary to achieve the purpose of the use, disclosure or request, except for:

a. Disclosures made to the Secretary of Health and Human Services
b. Uses or disclosures required by law
c. Uses or disclosures required for compliance with HIPAA

INTERNAL USES

1. The Privacy Officer will assess and determine, on a yearly basis, those Workforce Members who require access to PHI in order to carry out their job functions.
2. RioOne Health will document its Workforce Members' access to PHI in accordance with the Information Access Management Policy (HS-5).
3. The Privacy Officer will ensure that reasonable efforts are used to limit the access to the persons identified and for only the types of PHI which are needed to carry out their job functions.
4. For PHI that RioOne Health uses to perform certain management and administrative functions, RioOne Health will limit all uses of PHI to the minimum necessary to achieve the purpose of the particular management or administrative function.

EXTERNAL DISCLOSURES

1. For any disclosure that RioOne Health makes on a routine and recurring basis, RioOne Health will implement protocols that establish the minimum necessary amount of PHI that may be disclosed to achieve the purpose of the disclosure. On an annual basis, the Privacy Officer will:
    a. Assess and determine all routine and recurring disclosures requested or made by RioOne Health.
    b. Compose and complete a disclosure survey that identifies all routine and recurring disclosures.
    c. Assess and determine the types of PHI that are disclosed for the disclosures identified on the disclosure survey.
    d. For all recurring disclosures identified in the disclosure survey, the PHI disclosed will be limited to the amount reasonably necessary to achieve the purpose of the disclosure, but each disclosure does not require independent review by the Privacy Officer.
2. For all disclosures not specifically listed on the annual disclosure survey, the disclosure request must be sent to the Privacy Officer for review and determination for compliance with the minimum necessary standard.
3. Disclosures made to public officials as required by or in accordance with the law, if the public official represents that the information requested is the minimum necessary for the stated purpose(s), do not have to be reviewed by the Privacy Officer since they are deemed to be the minimum necessary for the requested disclosure.

Responsibility: Privacy Officer

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.514(d)(1)-(d)(3), Other Requirements Relating to Uses and Disclosures of PHI: Minimum Necessary Requirements

RioOne Health	HIPAA Privacy	Policy ID: HP-3
Title: **De-Identification of PHI**	Version: 1	Effective Date: **Draft**

HIPAA Privacy Rule Language: "Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information."

Purpose Statement: If permitted by the applicable Health Information Exchange Participants or Direct Messaging End User License Agreement or Business Associate Agreement, RioOne Health may use and disclose an individual's health information that has been de-identified. After health information is de-identified, it is no longer subject to the requirements of the HIPAA Privacy Regulations.

Policy/Procedure:

1. All de-identification of health information will be performed at the direction and under the supervision of the Privacy Officer and in accordance with the applicable Business Associate Agreement and Health Information Exchange Participants or Direct Messaging End User License Agreement.
2. The reason for the de-identification will be documented and maintained by the Privacy Officer.
3. RioOne Health may de-identify an individual's health information in either of the following ways:
    a. Remove all of the following identifiers from the individual's health information:
        i. Names.
        ii. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes.
        iii. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
        iv. Telephone numbers.
        v. Fax numbers.
        vi. Social Security numbers.
        vii. Electronic mail address.
        viii. Medical record numbers.
        ix. Health plan beneficiary numbers.
        x. Account numbers.
        xi. Certificate/license numbers.
        xii. Vehicle identifiers and serial numbers, including license plate numbers.
        xiii. Device identifiers and serial numbers.

xiv. Web Universal Resource Locators (URLs).
xv. Internet Protocol (IP) address numbers.
xvi. Biometric identifiers, including finger and voice prints.
xvii. Full face photographic images and any comparable images.
xviii. Any other unique identifying number, characteristic, or code, except as permitted for re-identification.

b. If any of the above 18 identifiers are not removed, RioOne Health may utilize a qualified person to determine that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify a subject of the information.

i. "qualified person" is a person:
   a. with appropriate knowledge and experience applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable;
   b. who applies such methods and principles to determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
   c. who documents the methods and results of the analysis that justify such determination.

4. No de-identified information will be disclosed if RioOne Health has knowledge that the information could be used alone or in combination to identify a subject of the information.
5. RioOne Health may assign a code or other means of record identification to allow information that has been de-identified to be re-identified by RioOne Health, as long as:
   a. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual.
   b. RioOne Health does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

Responsibility: Privacy Officer

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.514(a)-(c), De-Identification

RioOne Health	HIPAA Privacy	Policy ID: HP-4
Title: **Access of Individuals to PHI**	Version: 1	Effective Date: **Draft**

HIPAA Privacy Rule Language: "Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set."

Purpose Statement: RioOne Health does not create nor maintain designated record sets on behalf of its RioOne Health Information Exchange Participants or Health Direct Users. Therefore, RioOne Health cannot, on behalf of its RioOne Health Information Exchange Participants or Health Direct Users, grant an individual access to PHI. This policy sets forth how RioOne Health shall comply with requests from an individual to inspect or obtain a copy of his or her protected health information.

Policy/Procedure:

1. An individual who inquires about requesting his or her PHI will be provided a letter which indicates that RioOne Health does not maintain the individual's designated record set and cannot comply with the request.
2. The individual will be instructed to contact his or her health care provider(s) to request access to PHI contained within his or her medical record.
3. The following is template language for a response letter:

On [*insert date*], RioOne Health received a request from you for [*a copy of or the right to access*] protected health information about you that may have been exchanged through RioOne Health. RioOne Health is not a custodian of records nor does it maintain a designated record set. As a result, RioOne Health cannot provide you with the requested information. If you would like to access or obtain a copy of your health information, you should contact your health care provider(s) directly and they will gladly assist you.

Responsibility: Privacy Officer

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.524, Access of Individuals to PHI [Standard; Required]

RioOne Health	HIPAA Privacy	Policy ID: HP-5
Title: **Amendment of PHI**	Version: 1	Effective Date: **Draft**

HIPAA Privacy Rule Language: "An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set."

Purpose Statement: RioOne Health does not create nor maintain designated record sets on behalf of its RioOne Health Information Exchange Participants or Health Direct Users. Therefore, RioOne Health cannot, on behalf of its RioOne Health Information Exchange Participants or Health Direct Users, amend any protected health information. This policy sets forth how RioOne Health shall comply with requests from an individual to amend his or her protected health information.

Policy/Procedure:

1. In the event that RioOne Health receives a request from an individual to amend PHI exchanged through the Network, the individual will be provided with a letter which indicates that RioOne Health does not maintain medical records and cannot comply with the request to amend his or her medical record.
2. The individual will be instructed to contact his or her health care provider to request an amendment of his or her PHI.
3. The following is template language for a response letter:
   - On [*insert date*], RioOne Health received a request from you to amend protected health information about you that may have been exchanged through RioOne Health. RioOne Health is not a custodian of records nor does it maintain a designated record set. As a result, RioOne Health cannot make the requested amendment. If would like to amend your protected health information, you should contact your health care providers directly and they will gladly assist you.
4. RioOne Health shall maintain a log of all requests for amendments made directly to RioOne Health.

Responsibility: Privacy Officer

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.526, Amendment of Protected Health Information [Standard; Required]

RioOne Health	HIPAA Privacy	Policy ID: HP-6
Title: **Accounting of Disclosures of PHI**	Version: 1	Effective Date: **Draft**

HIPAA Privacy Rule Language: "An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested."

HITECH Act Language: "In applying section 164.528 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information—

> "(A) the exception under paragraph (a)(1)(i) of such section [treatment, payment, and health care operations] shall not apply to disclosures through an electronic health record made by such entity of such information; and
>
> "(B) an individual shall have a right to receive an accounting of disclosures described in such paragraph of such information made by such covered entity during only the three years prior to the date on which the accounting is requested."

"In response to a request from an individual for an accounting, a covered entity shall…provide an accounting, as specified under paragraph (1), for disclosures of protected health information that are made by such covered entity and by a business associate acting on behalf of the covered entity."

Purpose Statement: Individuals have a right to receive an accounting of disclosures of their protected health information made for the six years prior to their request. Pursuant to the RioOne Health Information Exchange Participants or Health Direct Messaging End User License Agreement, RioOne Health Information Exchange Participants or Health Direct Users are responsible for maintaining all information related to disclosures that the RioOne Health Information Exchange Participants or Health Direct User makes through RioOne Health Information Exchange Participants or Health Direct Messaging that will be needed to respond to a request for an accounting of disclosures. RioOne Health will only be responsible for providing information in response to a request for an accounting of disclosures for disclosures that RioOne Health makes, as permitted by the Business Associate Addendum or the RioOne Health Information Exchange Participants or Health Direct Messaging End User License Agreement.

Policy/Procedure:

REQUESTS FOR ACCOUNTING MADE TO COVERED ENTITIES

1. Within sixty (60)days of receiving the accounting request from the RioOne Health Information Exchange Participants or Health Direct User, RioOne Health will provide the RioOne Health Information Exchange Participants or Health Direct User with an

accounting of all disclosures of that individual's PHI made by RioOne Health during the six years (or such shorter time period as requested by the individual) prior to the request.

2. If RioOne Health is unable to act on the accounting request within sixty (60) days, RioOne Health may extend the deadline by no more than thirty (30) additional days if, prior to the expiration of the initial sixty (60) days, RioOne Health provides the RioOne Health Information Exchange Participants or Health Direct User with an explanation for the delay and an estimated date of completion. The RioOne Health Information Exchange Participants or Health Direct User will then notify the individual of the reason for the delay. RioOne Health may exercise only one such extension.

3. The content of the accounting provided to the RioOne Health Information Exchange Participants or Health Direct User will consist of the same information as provided below for accounting requests made directly to RioOne Health. In addition, the procedures regarding Exceptions and Suspensions provided below apply regardless of whether the RioOne Health Information Exchange Participants or Health Direct User submits the accounting request to RioOne Health or the individual submits the request directly to RioOne Health.

REQUEST FOR ACCOUNTING MADE BY INDIVIDUALS DIRECTLY TO RIOONE HEALTH

1. An individual may request an accounting of all disclosures pertaining to the individual's PHI made by RioOne Health to a third party during the six years prior to the request with the exception of those disclosures identified below. The individual may request an accounting for a period less than six years.

2. RioOne Health must act on an individual's request for an accounting within sixty (60) days of receiving the request. If RioOne Health is unable to act on the request within 60 days, RioOne Health may extend the deadline by no more than thirty (30) additional days if, prior to the expiration of the initial sixty (60) days, RioOne Health provides the individual with an explanation for the delay and an estimated date of completion. RioOne Health may exercise only one such extension.

3. Accounting requests will be delivered to the Privacy Officer who may designate another RioOne Health Workforce Member to process the request.

4. RioOne Health must provide the first accounting that an individual requests in a twelve (12) month period at no cost. RioOne Health may charge a reasonable cost-based fee for subsequent accountings requested in the same twelve (12) month period. RioOne Health must notify the individual of the cost requirement and allow the individual to withdraw or narrow the scope of his or her request to limit the cost of a subsequent accounting.

REQUIRED INFORMATION

1. The accounting must include all disclosures pertaining to the individual's PHI made by RioOne Health to a third party during the six years (or such shorter time period as requested by the individual) prior to the request, unless an exception applies.

2. For each disclosure, the following information must be included:
   a. The date of the disclosure.
   b. The name and address, if known, of the recipient of the PHI.
   c. A brief description of the PHI disclosed.
   d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure. Alternatively,

RioOne Health may include a written request from the third party for the information disclosed.

EXCEPTIONS

1. The following disclosures of PHI are not required to be included in a requested accounting:
   a. Disclosures made to carry out treatment, payment, and health care operations.
   b. Disclosures made to individuals of PHI about them.
   c. Disclosures made incident to a use or disclosure otherwise permitted or required by HIPAA.
   d. Disclosures made pursuant to an authorization.
   e. Disclosures made for the Covered Entity's facility directory or to persons involved in the individual's care.
   f. Disclosures made for national security or intelligence purposes.
   g. Disclosures made to correctional institutions or law enforcement officials.
   h. Disclosures made as part of a limited data set.
   i. Disclosures that occurred 6 years prior to the request.

SUSPENSION OF AN INDIVIDUAL'S RIGHT TO AN ACCOUNTING

RioOne Health must suspend an individual's right to receive an accounting of disclosures made to a health oversight or law enforcement agency if that agency requests that RioOne Health do so.

a. The agency requesting suspension must submit a written statement that RioOne Health's provision of a requested accounting to an individual would be reasonably likely to impede the activities of the agency. The statement must also state the duration of the requested suspension.

b. If the agency requesting suspension does not submit a written statement, but rather requests the suspension orally, RioOne Health must:

i. Document the identity of the agent and agency requesting the suspension and the reason for it. RioOne Health will include the badge number or a copy of the agent's credentials in the documented record.

ii. Effect a temporary suspension of the individual's right to an accounting of disclosures made to that agency.

iii. Limit the duration of the suspension to thirty (30) days or less from the time of the oral request, unless a written request is provided during that time.

DOCUMENTATION AND RETENTION

RioOne Health must retain the following documents for at least six years:

a. The information required to be included in a requested accounting.

b. Copies of written accountings provided to individuals.

c. Designation of persons responsible for processing requests for accountings made by individuals.

Responsibility: Privacy Officer; RioOne Health Information Exchange Participants or Health Direct User

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.528, Accounting of Disclosures of Protected Health Information [Standard; Required]
- Texas HB-300

RioOne Health	HIPAA Privacy	Policy ID: HP-7
Title: **Assigned Privacy Responsibility**	Version: 1	Effective Date: **Draft**

HIPAA Privacy Rule Language: "A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity."

Purpose Statement: **RioOne Health shall designate** a Privacy Officer who shall be responsible for the implementation and day-to-day administration and oversight of RioOne Health's compliance with the HIPAA Privacy Regulations. The Privacy Officer will also develop Workforce Member and User training programs regarding the privacy of PHI, update and implement these Privacy Policies and Procedures, and serve as the designated decision-maker for issues and questions involving interpretation of the HIPAA Privacy Regulations.

Policy/Procedure:

1. The Privacy Officer is responsible for the following tasks:
    a. Inventorying the uses and disclosures of all PHI;
    b. Ensuring that legal issues in drafting compliance documents are addressed or engage competent legal counsel to draft such documents;
    c. Administering sanctions upon Workforce Members for violations of these Privacy Policies and Procedures;
    d. Developing, updating, and revising these Privacy Policies and Procedures as necessary to comply with the HIPAA Privacy Regulations;
    e. Developing a privacy training program for Workforce Members and Users;
    f. Establishing procedures to monitor internal privacy compliance;
    g. Keeping up to date on the latest privacy developments and federal and state laws and regulations;
    h. Coordinating with the Security Officer in evaluating and monitoring operations and systems development for Privacy and Security requirements;
    i. Serving as RioOne Health's liaison to regulatory bodies for matters relating to privacy
    j. Coordinating any audits of the Secretary of HHS or any other governmental or accrediting organization regarding RioOne Health's compliance with state or federal privacy laws or regulations; and
    k. Other tasks that is necessary to ensure the privacy of PHI.
    l. Complying with HIPAA, HITECH and Texas law on disposal of PHI.
    m. Performing initial and periodic risk assessments or "privacy audits" and conducting ongoing compliance monitoring activities.
    n. Reviewing all system-related information security plans in order to align

security and privacy practices.

o. Guiding and assisting in the identification, implementation, and maintenance of privacy policies and procedures in coordination with RioOne Health's management, RioOne Health Participants and legal counsel.
p. Conducting, at least annually, a review of RioOne Health's access procedures for individuals.

The above list provides an overview of the RioOne Health Privacy Officer duties and is not meant to serve as an all-inclusive list.

2. RioOne Health's Privacy Officer's name and contact information is:
   Name: Charles C. Stewart
   Email: c.stewart@dhr-rgv.com
   Subject line: Privacy@RioOneHealth
   Phone (work): (956) 362-3058
   Phone (cell): (832) 439-8810

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.530(a), Personnel Designations [Standard; Required]

RioOne Health	HIPAA Privacy	Policy ID: HP-8
Title: **Right of an Individual to Request Restriction of Uses and Disclosures**	Version: 1	Effective Date: **Draft**

PURPOSE:
To clarify that participation with RioOne Health is based on authorization signed by individuals agreeing to allow use and disclosure of all his/her PHI to and through the Exchange. PHI subject to restrictions will not be transferred through the Exchange by Participants.

POLICY:
1. RioOne Health will not restrict use and disclosure of an individual's PHI.
2. Because RioOne Health will not segment PHI in the Exchange, upon notice from a Participant that he/she has agreed to a restriction, RioOne Health will initiate procedures to shut down further use or disclose of that individual's PHI through the Exchange.
3. In the event RioOne Health receives a request to restrict use and disclosure of PHI directly from an individual, RioOne Health will forward the written request, or refer the patient who calls with such a request, to the Participant.
4. RioOne Health shall maintain a log of all such requests for restrictions.

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations

Regulatory Reference:
- 45 C.F.R. §164.502(c) 45 CFR 164.522(a) as amended by HITECH Act §13405(a) and NPRM dated July 14, 2010

RioOne Health	HIPAA Privacy	Policy ID: HP-9
Title: **Privacy Complaint Violation**	Version: 1	Effective Date: **Draft**

PURPOSE:
To implement a procedure for receiving, documenting, and taking appropriate action with respect to privacy complaints.

POLICY:
1. All Privacy Complaints must be submitted to the RioOne Health Privacy Officer or his/her designees.

2. Privacy Complaints must include a statement that describes the basis of the complaint.

3. The RioOne Health Privacy Officer will determine what health care information the individual claims was misused or improperly disclosed. If the health care information at issue was created or maintained by a Participant or a Business Associate, the complaint will be forwarded to the Participant or Business Associate.

Responsibilities Of The RioOne Health Privacy Officer
1. The Privacy Officer shall determine:
   A. Whether there has been a violation of the privacy regulations or RioOne Health's privacy policies.
   B. What, if any, internal privacy practices need to be changed.
   C. What, if any, additional policies need to be developed.
   D. What additional training will be provided to the person who violated the privacy regulations or policies.

2. The Privacy Officer will determine whether a violation has occurred and will determine appropriate sanctions.

3. The Privacy Officer shall document all complaints received by RioOne Health and the action taken in response to the complaint in a separately and confidentially maintained individual complaint file. Documentation of each complaint will be retained in written or electronic form.

Responsibility: Privacy Officer

Regulatory Category: Privacy Regulations

Regulatory Reference: 45 CFR 164.530

It is the responsibility of each Workforce member to comply with these policies, procedures, and applicable Texas and Federal confidentiality laws and regulations. Any concerns or questions regarding this policy should be directed to the Privacy Officer.

A. Workforce Member's Duty to Report Violations of Policies.

1. Any Workforce member who observes or is aware of a PHI policy violation must report the violation to the Privacy Officer.
2. Any Workforce member who believes in good faith that a violation of PHI policy has occurred may report such violation to RioOne Health without violating this policy. RioOne Health will not intimidate, threaten, coerce, discriminate against, or take retaliatory action against any individual who reasonably exercises his/her rights under this policy.
3. Failure to report a violation of RioOne Health's PHI policies is a violation of this policy and may lead to disciplinary action, up to and including termination.

B. Disciplinary Action.

1. Failure to comply with PHI policies may be grounds for disciplinary action, including termination of employment. The appropriate level of disciplinary action will be determined on a case by case basis, taking into consideration the specific circumstances and severity of the violation. In cases where disciplinary action is imposed (except termination), the Workforce member shall be required to repeat confidentiality training.
2. The following is a partial list of Workforce member conduct that will constitute a violation of the PHI policies and thus lead to disciplinary action, up to and including termination. There may be other conduct that is not listed which would also constitute policy violations.
3. ***Workforce Member:***

A. Demonstrates a pattern or practice of discussing individual information in a public area;

B. Demonstrates a pattern or practice of leaving a record in a public area;

C. Demonstrates a pattern or practice of leaving a computer containing PHI unsecured;

D. Looks up an individual's address or relative's address for personal rather than legitimate and authorized business and claim purposes;

E. Compiles a mailing list with the intent to sell or use for personal purposes; and

F. Reviews or discloses PHI in order to advance a personal cause of action.

C. Explanation of Disciplinary Actions.

RioOne Health generally will follow a progressive discipline policy as set forth below in imposing discipline for violations of this policy. However, RioOne Health reserves the

right, in appropriate circumstances, to immediately terminate or otherwise discipline an employee without notice and/or without following the progressive discipline steps.

1. Oral Counseling:

a. Though the counseling is oral, the counseling should be documented.
b. The record should indicate that it is a verbal counseling.
c. The Workforce member should sign the form.
d. A refusal to sign should be indicated on the form.

2. Written Counseling:

a. This counseling is to be documented.
b. The Workforce member should sign the form.
c. A refusal to sign should be indicated on the form.

3. Termination: The reasons for discharge should be documented and discussed with the Workforce member.

D. Mitigation. In an effort to protect all PHI, RioOne Health will mitigate, to the extent practicable, any harmful effect that results from a **known** use or disclosure of PHI in violation of the PHI policies.

E. No Retaliation. Individuals shall be protected from retaliation if they act in good faith in the belief that the opposed behavior is unlawful, the manner of the opposition is reasonable and does not involve the disclosure of PHI in violation of the rule. Further, RioOne Health shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for filing a complaint; testifying, assisting, or participating in an investigation or compliance review; or opposing any act or practice made unlawful by RioOne Health's privacy policies or by Texas and Federal laws.

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.530(a), Personnel Designations [Standard; Required]

HIPAA Security
Policies and Procedures

RioOne Health	HIPAA Security	Policy ID: HS-1
Title: **IT Security and Risk Management, Evaluation and Updates**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language:
"Implement policies and procedures to prevent, detect, contain, and correct security violations."

"Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic PHI that establishes the extent to which an entity's security and procedures meet the requirements of this subpart."

"Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information."

Purpose Statement: RioOne Health, under the HIPAA Security Regulations, is required to periodically evaluate its security safeguards and implement an IT security and risk management process. Implementation of this IT security and risk management process will assist RioOne Health in ensuring the confidentiality, integrity, and availability of ePHI and the Network. RioOne Health will create and maintain appropriate and reasonable policies, procedures, and controls to prevent, detect, contain, and correct security violations.

Policy/Procedure:

EVALUATION AND RISK ANALYSIS

3. At least once per year, RioOne Health will convene a workgroup of at least four (4) individuals to conduct an accurate and thorough evaluation of RioOne Health's security safeguards and an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI accessed through the Network.
4. The workgroup will consist of at least the Security Officer, individuals representing RioOne Health's information technology department or RioOne Health's technology vendor, individuals familiar with the Network and legal counsel for RioOne Health.
5. The workgroup will conduct the following activities:
    a. A review of RioOne Health's IT Security and Risk Management Policies and Procedures to evaluate their appropriateness and effectiveness in protecting against any reasonably anticipated threats or hazards to the privacy and security of ePHI exchanged through the Network.
    b. A gap analysis to compare RioOne Health's IT Security and Risk Management Policies and Procedures against actual practices.

c. An identification of threats and risks to the Network ("Risk Analysis"), including the following:

i. Potential security risks to the Network, including those Security Incidents specifically identified in the Breach and Security Incident and Response Procedures Policy (H-4);

ii. The probability of the occurrence of risks which may affect the Network;

iii. The magnitude of the identified risk to the Network;

iv. The criticality of each Network function to RioOne Health's operations during or after an emergency or disaster pursuant to the Applications and Data Criticality Analysis Policy (HS-15);

v. The frequency of reviews and audits of the Network pursuant to the Information System Activity Review Policy (HS-2);

vi. The training, and the frequency of such training, to be offered to RioOne Health Information Exchange Participants or Health Direct Users and Workforce Members regarding the security of ePHI;

vii. The need to do penetration testing of the security of the Network; and

viii. The need to engage third parties to evaluate the risks and vulnerabilities to the Network.

d. An assessment of whether established security controls reasonably and appropriately protect against the risks identified for the Network.

4. The evaluation and risk analysis process will be documented and the findings will be reported to the RioOne Health Governing Body.

RISK MANAGEMENT

1. In an effort to reduce risks and vulnerabilities to ePHI exchanged through the Network, RioOne Health will update its IT Security and Risk Management Policies and Procedures if the results of the evaluation show that such updates are needed and will create a Risk Management Plan to address risks identified in the annual Risk Analysis.

2. In addition to updating the IT Security and Risk Management Policies and Procedures after each Risk Analysis, RioOne Health will also update the Policies and Procedures and Plan as needed:

a. After any Security Incident to minimize the likelihood of a similar Security Incident occurring in the future;

b. After a new use of the Network is authorized;

c. In response to the addition of any new Network functionality;

d. In response to environmental or operational changes (e.g. significant new threats or risks to the security of ePHI; changes to RioOne Health's organizational or technical infrastructure; changes to information security requirements or responsibilities; or availability of new security technologies or recommendations).

3. In developing each Risk Management Plan, RioOne Health will consider the following:

a. The security measures that are already in place to address the risk;

b. Additional security measures that can reasonably and appropriately be put in place to address the risk;

c. Communication of the security measures and Risk Management Plan to Workforce Members, RioOne Health Information Exchange Participants or Health Direct Users, and Vendors; and

d. The need to engage other resources to assist in the implementation of the Risk Management Plan.

Responsibility: Security Officer

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(1)(i), Security Management Process [Standard; Required]
- 45 C.F.R. §164.308(a)(1)(ii)(A), Risk Analysis [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(1)(ii)(B), Risk Management [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(8), Evaluation [Standard; Required]
- 45 C.F.R. §164.316(b)(2)(iii), Updates [Implementation Specification; Required]

RioOne Health	HIPAA Security	Policy ID: HS-2
Title: **Information System Activity Review**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Purpose Statement: RioOne Health will implement hardware, software, and/or procedural mechanisms that record and examine the activity of Users in the Network to enable RioOne Health to detect potentially problematic activity in the Network. These audit controls will allow RioOne Health to:

1. Identify questionable access to and exchange activities in the Network;
2. Investigate Breaches and Security Incidents;
3. Respond to potential weaknesses in the Network's architecture; and
4. Assess the effectiveness of RioOne Health IT Security and Risk Management Policies and Procedures.

FREQUENCY OF THE NETWORK ACTIVITY REVIEW

1. RioOne Health will conduct monthly audits, and create audit reports, which provide a summary of all uses of the Network.
2. RioOne Health will identify and document the names of Workforce Members who will review monthly audit reports.
3. RioOne Health will retain monthly audit reports for six (6) years after the date they are created.

AUDIT REPORT CONTENT

1. For each Network service, RioOne Health will identify the data to be captured in the monthly audit reports. The data to be captured in monthly audit reports related to RioOne Health Information Exchange Participants or Health Direct Messaging is set forth in RioOne Health Information Exchange Participants or Health Direct Messaging Auditing and Monitoring Policy (DM-7).
2. Within two weeks of receiving the monthly audit report, a designated RioOne Health Workforce Member will review the report.
3. If RioOne Health uncovers any indications of improper use of the Network, it will follow the Breach and Security Incident Response Procedures Policy (H-4).
4. As patterns are identified and anomalous behavior becomes more apparent in the monthly audit reports, RioOne Health may establish thresholds for each type of activity captured in the audit report. The thresholds will signify the level at which certain behavior

warrants further inspection and may signal a Breach or Security Incident or failure to comply with RioOne Health's policies and procedures. As thresholds are established or revised, this Policy or other related Policies will be revised accordingly.

Responsibility: Security Officer

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164308(a)(1)(ii)(D), Information System Activity Review [Implementation Specification; Required]
- 45 C.F.R. §164.312(b), Audit Controls [Standard; Required]

RioOne Health	HIPAA Security	Policy ID: HS-3
Title: **Assigned Security Responsibility**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."

Purpose Statement: Under the HIPAA Security Regulations and the HITECH Act, RioOne Health is required to designate a Security Official who is responsible for the development and implementation of its Security Policies and Procedures. This policy reflects RioOne Health's commitment to comply with such regulations. In addition, the appointment of the Security Officer will provide organizational focus to, and highlight the importance of, RioOne Health's efforts to protect the confidentiality, privacy and security of the ePHI.

Policy/Procedure:

1. The Security Officer shall perform the following duties, including taking all reasonable and appropriate measures to:
    a. Ensure and confirm that RioOne Health is compliant with applicable federal, state, and local laws pertaining to the security of ePHI;
    b. Guide the development, documentation, and dissemination of appropriate security policies and procedures that govern the use of the Network;
    c. Ensure that any updates to the Network have options that support required and/or addressable implementations of the HIPAA Security Regulations and RioOne Health's internal security requirements;
    d. Approve and oversee the administration, implementation, and selection of RioOne Health's security controls for the Network;
    e. Implement and oversee the security training of Users, and ensure that Users receive such training on a periodic basis as deemed necessary pursuant to RioOne Health's IT Security and Risk Management, Evaluation and Updates Policy (HS-1);
    f. Facilitate the yearly Risk Analysis and creation of a Risk Management Plan under RioOne Health's IT Security and Risk Management, Evaluation and Updates Policy (HS-1);
    g. Ensure that the Network activity is monitored and audited to identify Security Incidents and malicious activity as set forth in the Information System Activity Review Policy (H-2);
    h. Ensure that the threats and risks to the confidentiality, integrity, and availability of ePHI are monitored and evaluated; and
    i. Oversee the development and implementation of an effective Security Incident response policy and related procedures as set forth in the Breach and Security Incident Management and Response Procedures Policy (H-4).

2. RioOne Health's Security Officer is
   Name: Charles C. Stewart
   Email: c.stewart@dhr-rgv.com
   Subject line: Security@RioOneHealth
   Phone (work): (956) 362-3058
   Phone (cell): (832) 439-8810

Note: This person can be the same as the Privacy Officer

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(2), Assigned Security Responsibility [Standard; Required]

RioOne Health	HIPAA Security	Policy ID: HS-4
Title: **Workforce Member Security**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI, as provided under paragraph (a)(4) [information access management] of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic PHI."

Purpose Statement: To protect the confidentiality, integrity, and availability of ePHI, RioOne Health will implement reasonable and appropriate safeguards to prevent unauthorized access to ePHI while ensuring that properly authorized Users can exchange ePHI through the Network.

Policy/Procedure:

WORKFORCE CLEARANCE

1. Security privileges will be identified and defined for each Workforce Member who is granted access to the Network.
2. Based on the level of privileges to be granted to candidates for employment, Human Resources personnel will perform appropriate and reasonable verifications checks on the candidate.
3. Verification checks may include, but are not limited to:
    a. Character references;
    b. Confirmation of claimed academic and professional qualifications;
    c. Credit checks; or
    d. Criminal background checks.
4. Upon accepting an offer of employment, each Workforce Member who will have access to the Network will sign the Workforce Member Confidentiality and Compliance Statement as required pursuant to the Workforce Member Confidentiality and Compliance Statement Policy (H-2).

SUPERVISION OF WORKFORCE MEMBERS

1. The Security Officer will take reasonable and appropriate steps to ensure that Workforce Members, who have the ability to access the Network, or those who work in areas where ePHI might be accessed, will be properly supervised. RioOne Health will ensure that Workforce Members only access the ePHI that they are authorized to access pursuant to their job responsibilities.
2. RioOne Health will ensure that appropriate sanctions are taken against Workforce Members who improperly access ePHI, or who inappropriately grant access to ePHI to others. Sanctions will be instituted in accordance with the RioOne Health Workforce Member Discipline Policy.

Confidentiality Agreement: Each Workforce member, full-time employee, temporary employee, consultant, contracted employee, subcontractor, vendor, and business associate shall be required to sign a confidentiality agreement or, where applicable, a business associate agreement, upon commencing work or entering into a contractual relationship with RioOne Health.

A. All Workforce members, as a condition of employment, are required to sign the confidentiality agreement.

B. Copies of the agreement shall be maintained in the Workforce member's personnel file.

C. Where required by HIPAA or Texas law, contractors who meet the definition of a business associate shall be required to execute a business associate or chain of trust partner agreement. All other contractors must sign a confidentiality agreement if the service involves the incidental use or disclosure of PHI.

ACCESS TO ePHI

RioOne Health will authorize, establish and modify, as appropriate, each Workforce Member's access to ePHI in accordance with the Information Access Management Policy (HS-5).

TERMINATION OF ACCESS TO ePHI

RioOne Health will terminate a Workforce Member's access to ePHI, either in the event of a Workforce Member's resignation or a Workforce member's termination by RioOne Health, in accordance with the Suspension and Termination Procedures Policy (HS-6).

Responsibility: Security Officer; Human Resources; Workforce Members

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(3)(i), Workforce Security [Standard; Required]
- 45 C.F.R. §164.308(a)(3)(ii)(A), Authorization and/or Supervision [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(3)(ii)(B), Workforce Clearance Procedure [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-5
Title: **Information Access Management**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of subpart E of this part."

Subpart E refers to the HIPAA Privacy rules, located at 45 C.F.R. §164.500 et seq.

Purpose Statement: RioOne Health strives to protect the confidentiality, integrity, and availability of ePHI by taking reasonable steps to appropriately manage access to the Network. Safeguarding access to the Network by taking reasonable and appropriate steps is integral to RioOne Health's compliance efforts under the HIPAA Security Regulations.

Policy/Procedure:

ESTABLISHING ACCESS TO ePHI FOR RIOONE HEALTH WORKFORCE MEMBERS

1. RioOne Health will ensure that only authorized Workforce Members will have access to the Network.
2. RioOne Health will document the various levels of access to the Network that each Workforce Member will have based upon the job function requirements of each position.
3. Workforce Members will not be granted access to, and must not attempt to access, the Network until the Workforce Member has been properly cleared in accordance with the Workforce Member Security Policy (HS-4).
4. Once a Workforce Member has been granted access to the Network, the Security Officer will give notice of such access to the RioOne Health Systems Administrator, or designee.
5. The Systems Administrator, or designee, will then assign the Workforce Member a unique username and temporary password to activate the Workforce Member's level of access to the Network.
6. Once the Workforce Member receives his or her temporary password, the Workforce Member will change his or her password in accordance with the Password Management Policy (HS-11).

REVIEW AND MODIFICATION OF WORKFORCE MEMBERS' ACCESS TO ePHI

1. RioOne Health will periodically review Workforce Members' access privileges to the Network.
2. RioOne Health may modify, if necessary, a Workforce Member's access privileges to the Network.
    a. When a Workforce Member's access to the Network must be modified, either because of a change in the Workforce Member's job function or the Workforce Member's termination, RioOne Health will document such modifications.

b. Such documentation may include:

i. The date and time of the modification;
ii. The identification of the Workforce Member whose access is being modified;
iii. A description of the Workforce Member's modified access rights; and
iv. The reason for the modification of the Workforce Member's access rights.

ACCESS TO RIOONE HEALTH INFORMATION EXCHANGE OR HEALTH DIRECT MESSAGING FOR RIOONE HEALTH DIRECT USERS

1. Individuals will be provided with access to RioOne Health Information Exchange or Health Direct Messaging in accordance with RioOne Health Information Exchange or Health Direct Messaging User Enrollment Policy (DM-8).

Responsibility: Security Officer; Systems Administrator (or designee); RioOne Health Direct Users

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(4)(i), Information Access Management [Standard; Required]
- 45 C.F.R. §164.308(a)(4)(ii)(B), Access Authorization [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(4)(ii)(C), Access Establishment and Modification [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-6
Title: **Suspension and Termination Procedures**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement procedures for terminating access to electronic PHI when the employment of a workforce member ends or as required by determinations as specified in paragraph (a)(3)(ii)(B) [workforce clearance] of this section."

Purpose Statement: When a Workforce Member's employment ends or the Workforce Member's access to ePHI is no longer appropriate, RioOne Health will terminate the Workforce Member's access to ePHI.

Policy/Procedure:

TERMINATION PROCEDURES UPON A WORKFORCE MEMBER'S RESIGNATION

1. When a Workforce Member provides notice of his or her intention to end employment with RioOne Health, the Human Resources Manager and the Workforce Member's supervisor will give reasonable notice to the RioOne Health Systems Administrator (or designee), so that the departing Workforce Member's access to the Network can be terminated when he or she ends employment.
2. RioOne Health will document the following information regarding the departing Workforce Member:
    a. Date and time of receiving the Workforce Member's notice to end employment at RioOne Health;
    b. Date of the Workforce Member's planned departure;
    c. Description of the Workforce Member's access to the Network that must be terminated; and
    d. Date, time, and description of the actions taken to terminate the departing Workforce Member's access to the Network.

TERMINATION PROCEDURES UPON A WORKFORCE MEMBER'S TERMINATION BY RIOONE HEALTH

1. When a Workforce Member is terminated, RioOne Health will immediately remove or disable the Workforce Member's access privileges to the Network before the Workforce Member is notified of his or her termination, when feasible.
2. Such Network access privileges include, but are not limited to:
    a. Workstations and server access;
    b. Access to data contained within or available through the Network;
    c. Access to any network that RioOne Health uses;
    d. Email accounts; and/or
    e. Inclusion on group email lists.

GENERAL RESIGNATION AND TERMINATION PROCEDURES

1. RioOne Health will terminate, as appropriate, a departing or terminated Workforce Member's physical access to areas where ePHI is located within RioOne Health's facilities.
2. RioOne Health will collect, and document the collection of, equipment and property that contains ePHI, which were used by the terminated or departing Workforce Member.
    a. Such documentation will include:
        i. The Workforce Member's name;
        ii. The date and time the equipment and property were returned; and
        iii. The identification of the returned property and equipment.
    b. RioOne Health will securely maintain such documentation.
3. Equipment that may contain, allow, or enable the Workforce Member to access ePHI, and which must be returned upon the workforce member's termination or departure, include, but is not limited to:
    a. Portable computers;
    b. Personal Digital Assistants (PDAs);
    c. Name tags or name identification badges;
    d. Security tokens;
    e. Facility access cards; and/or
    f. Building, desk, or office keys.

SUSPENSION AND TERMINATION PROCEDURES FOR RIOONE HEALTH DIRECT USERS

1. RioOne Health Information Exchange or Health Direct Users may be suspended or terminated in accordance with the RioOne Health Information Exchange or Health Direct Messaging End User License Agreement and the RioOne Health Information Exchange or Health Direct User Suspension and Termination Policy (DM-9).

Responsibility: Security Officer; Systems Administrator (or designee); Human Resources Manager

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(3)(ii)(C), Termination Procedures [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-7
Title: **Security Awareness and Training**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement a security awareness and training program for members of its workforce (including management)."

Purpose Statement: RioOne Health has the responsibility under the HIPAA Security Regulations for providing and documenting security awareness and training for RioOne Health Workforce Members in order that those persons can properly carry out their functions while appropriately safeguarding ePHI. This policy reflects RioOne Health's commitment to comply with such Regulations.

Policy/Procedure:

TRAINING FOR WORKFORCE MEMBERS

1. RioOne Health will provide customized training and supporting reference materials to its Workforce Members, as appropriate, to carry out their functions with respect to the security of ePHI. As part of its risk analysis, pursuant to its IT Security and Risk Management, Evaluation and Updates Policy (HS-1), RioOne Health will determine how often such training will be required for its Workforce members and the method of such training. Training at a minimum will be conducted every two years.
2. RioOne Health will maintain sufficient records that document and confirm a Workforce Member's completion of security awareness training by a given deadline date, such as a document signed by each Workforce member and the Security Officer acknowledging receipt of such training.
3. Security awareness training should include information to make Workforce Members aware of and familiar with RioOne Health's HIPAA Security Policies and Procedures and Texas HB-300 rules.
4. RioOne Health will provide security information reminders and updates to its Workforce Members, in accordance with the Security Reminders Policy (HS-8).
5. RioOne Health will make its Security Policies and Procedures available for reference and review by its Workforce Members who have access to ePHI.

Responsibility: Security Officer

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(5)(i), Security Awareness and Training [Standard; Required]
- Texas HB-300

RioOne Health	HIPAA Security	Policy ID: HS-8
Title: **Security Reminders**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement periodic security updates."

Purpose Statement: RioOne Health will periodically provide information and reminders to Users on a variety of topics designed to increase the security of the Network.

Policy/Procedure:

1. RioOne Health's Security Officer will periodically, as needed, issue security information and awareness reminders to Users. Such security reminders could include:
    a. Information regarding general security risks and how to follow RioOne Health's HIPAA Security Policies and Procedures;
    b. Information regarding how to use the Network in a manner that reduces security risks; and/or
    c. Legal and business responsibilities of RioOne Health for protecting the ePHI exchanged through the Network.
2. RioOne Health will issue security reminders immediately upon, or within a reasonable time following the occurrence of any of the following events:
    a. Making substantial revisions to RioOne Health's Security Policies and Procedures;
    b. Implementing new, or significantly changing existing, security controls;
    c. Making substantial changes to RioOne Health's legal or business responsibilities;
    d. Identifying substantial threats or new risks against the Network; or
    e. Introducing new functions or making significant changes to existing Network functionalities.
3. Means of providing security information and awareness reminders and updates may include, but are not limited to:
    a. Email reminders;
    b. Posters;
    c. Letters;
    d. Meetings;
    e. Information system sign-on messages;
    f. Newsletter articles; and/or
    g. Information posted to the Network.

Responsibility: Security Officer

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(5)(ii)(B), Security Reminders [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-9
Title: **Malicious Software**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement procedures for guarding against, detecting, and reporting malicious software."

Purpose Statement: RioOne Health will implement and periodically review its processes and safeguards for guarding against, detecting, and reporting malicious software that pose risks to privacy and security ePHI, or the integrity or operation of the Network.

Policy/Procedure:

1. RioOne Health will take all necessary and reasonable measures to protect the Network, and all media that RioOne Health uses upon which ePHI is contained, from malicious software, including:
    a. Ensuring that anti-virus software is installed on all media devices and hardware, either owned by or used by RioOne Health containing ePHI or which have access to the Network;
    b. Mitigating the harm of malicious software attacks by recovering ePHI and other data contained on all media devices and hardware that has been attacked by malicious software;
    c. Requiring all Workforce Members to scan email attachments and downloads before they are opened.
2. RioOne Health will conduct a weekly virus scan of its network server and Workstations.
3. RioOne Health Workforce Members must not bypass or disable anti-virus software installed on Workstations unless they are properly authorized to do so.
4. RioOne Health will provide periodic training and awareness to its Workforce Members about guarding against, detecting, and reporting malicious software, including:
    a. How to discover malicious software;
    b. How to report malicious software;
    c. How to scan for malicious software that may be contained in email attachments; and/or
    d. How to use anti-virus software.
5. Workforce Members must pass electronic files through virus protection programs prior to use, pursuant to the Malicious Software Policy (HS-9).
6. Workforce Members must immediately report suspected or confirmed malicious software to the Security Officer.

Responsibility: Security Officer; Systems Administrator or Designee; Workforce Members

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(5)(ii)(B), Protection from Malicious Software [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-10
Title: **Log-In Monitoring and Automatic Log-Off**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement procedures for monitoring log-in attempts and reporting discrepancies."

Purpose Statement: RioOne Health will control access to its Workstations through the use of log-in procedures and automatic log-off functionality. RioOne Health will use similar log-in monitoring and automatic log-off functionality for those components of the Network that are accessed through a web-based user interface.

Policy/Procedure:

LOG-IN MONITORING

1. After five consecutive, unsuccessful attempts to log-on to a RioOne Health Workstation, the Workforce Member's password will be disabled. All such events will be logged as part of the monthly activity report pursuant to the Information System Activity Review Policy (HS-2).
2. If a Workforce Member's password is disabled due to unsuccessful log-on attempts, the Workforce Member should contact the Systems Administrator, (Security Officer; or Designee).
3. The Systems Administrator will verify the Workforce Member's identity and determine whether the Workforce Member's access was disabled because of five consecutive, unsuccessful attempts to log-on or for another reason.
4. After verifying the Workforce Member's identity and that such Member's access was disabled because of unsuccessful log-on attempts, the Systems Administrator will issue the Workforce Member a new, temporary password. The Workforce Member will then use the temporary password to log-on to the Workstation and re-set his or her own individual password in accordance with the Password Management Policy (HS-11).

AUTOMATIC LOG-OFF

1. A Workforce Member will be automatically logged-off of a RioOne Health Workstation after 30 minutes of inactivity.
2. To activate a new session, a Workforce Member will have to log-on to the Workstation using his or her user name and password.

Responsibility: Security Officer; Workforce Members

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(5)(ii)(C), Log-In Monitoring [Implementation Specification; Addressable]
- 45 C.F.R. §164.312(a)(2)(iii), Automatic Log-off [Technical Safeguards; Implementation Specification for Device and Media Controls; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-11
Title: **Password Management**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement procedures for creating, changing, and safeguarding passwords."

Purpose Statement: Where RioOne Health requires the use of a password to access or exchange information through the Network, Users will be required to take appropriate measures to select and secure such passwords.

Policy/Procedure:
1. Passwords are case sensitive requiring at least 6 characters, (Alphanumeric: (1) Uppercase, (1) Lowercase, (1) Numeric), and (1) Special Character.
2. Users may not, under any circumstances, share their passwords or second method of authentication, if applicable, with anyone. If a User does share his/her password with another person, they must notify the Systems Administrator immediately so that the password can be re-set.
3. Users should refrain from recording or using passwords where they may be obtained or observed by others.

Responsibility: Security Officer; Systems Administrator; Users

Regulatory Category: Administrative Safeguards

Regulatory Reference:
- 45 C.F.R. §164.308(a)(5)(ii)(D), Password Management [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-12
Title: **Contingency Plan**	Version: 1	Effective Date: **Draft**

Purpose Statement: The RioOne Health Contingency Plan establishes IT Security and Risk Management Plan to recover the Network following a disruption. RioOne Health has established the following objectives for this Contingency Plan:

1. Maximize the effectiveness of RioOne Health's contingency operations through an established plan that consists of the following phases:
    a. Notification and Activation Phase to detect and assess damage and to activate the plan;
    b. Recovery phase to restore temporary Network operations and to recover damage done to the Network; and
    c. Reconstitution phase to restore the Network's functional capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out Network requirements during prolonged interruptions to normal operations.
3. Assign responsibilities to designated Workforce Members who will participate in the contingency planning strategies, and provide guidance for recovering the Network during prolonged periods of interruption to normal operations.
4. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

Policy/Procedure:

CONTINGENCY PLAN TRIGGERS

1. This Contingency Plan will be activated upon the occurrence of one or more of the following triggers:
    a. RioOne Health Information Exchange or Health Direct Messaging will be completely unavailable for more than 5 business hours due to an unplanned outage; and
    b. Other triggers, as appropriate.

MITIGATION MEASURES

1. RioOne Health will use at least a Tier 3 data center to house its servers. Because of the robust protections offered by a Tier 3 data center, the likelihood of damage to the Network is very low. If there is damage to the Network, RioOne Health will be able to recover exact copies of ePHI, to the extent that it is maintained within the Network, pursuant to the Data Back-Up and Disaster Recovery Plan Policy (HS-13).
2. RioOne Health will take various steps to mitigate any damage to the Network caused by an emergency or disaster and to continue operations after such an event. RioOne Health may perform these measures itself or may require that other third parties, to whom RioOne Health has outsourced certain activities, perform these measures.
    a. Ensure that preventative controls, such as generators, waterproof tarps,

sprinkler systems, and fire extinguishers will be fully operational at the time of an emergency or disaster.

b. Ensure that its electronic media and hardware containing ePHI, including components supporting such devices, are connected to an uninterruptible, redundant power supply.

c. Ensure that RioOne Health will maintain service agreements with its hardware, software, and communications providers to support Network recovery.

NOTIFICATION PROCEDURES

1. RioOne Health personnel or a third party representative who discovers that RioOne Health's facilities, the third party's facilities, or the Network has been affected by an emergency or disaster, must notify the appropriate RioOne Health official, by telephone, pursuant to the following:
    a. Privacy Officer: Charles C. Stewart (office): (956) 362-3058(cell): (832) 439-8810
    b. Security Officer: Charles C. Stewart (office): (956) 362-3058(cell): (832) 439-8810
    c. Technical Director: Charles C. Stewart (office): (956) 362-3058(cell): (832) 439-8810

2. When notified, the RioOne Health official will notify all others within RioOne Health who will be part of the contingency and recovery activities.

DAMAGE ASSESSMENT PROCEDURES

The Systems Administrator, or other RioOne Health Official, upon his or her initial review of the situation, will assess the following:

a. The cause of the disruption;
b. The potential for additional disruption or damage;
c. The affected physical area and the status of physical infrastructure;
d. The status of the Network server's functionality and inventory, including items that may need to be replaced; and
e. The estimated time to repair services to normal operations.

ACTIVATION OF CONTINGENCY PLAN

Based on the damage assessment from the Systems Administrator, or other RioOne Health Official, RioOne Health senior management will determine what contingency operations and recovery activities are necessary to repair and sustain operations of the Network.

RECOVERY OPERATIONS

RioOne Health will restore the Network and recover any ePHI that was maintained within the Network in accordance with the following Policies and Procedures:

a. Data Backup Plan and Disaster Recovery Plan Policy (HS-13); and
b. IT Security and Risk Management Plan (HS-14).

OTHER CONTINGENCY PLAN PROCEDURES

1. RioOne Health will perform a critical analysis of each Network function to determine its importance to RioOne Health's operations during or after a disaster in accordance with the IT Security and Risk Management, Evaluation and Updates Policy (HS-1) and as outlined in the Applications and Data Criticality Analysis Policy (HS-15).
2. RioOne Health will provide periodic training materials regarding its disaster and emergency response procedures to Workforce Members, as appropriate.
3. RioOne Health will periodically test its Contingency Plan to ensure that critical business processes can continue in a satisfactory manner. If necessary, RioOne Health may revise the Contingency Plan, and the occurrence of any of the following events may result in a revision of the Contingency Plan:
    a. Disaster recovery role and responsibility changes, including changes to contact information;
    b. Changes to RioOne Health's physical or technical infrastructure or operating systems;
    c. Changes in threats to the Network; or
    d. Results of testing that indicate that the plan needs to be modified to ensure that it is sufficient, accurate, and up-to-date.

Responsibility: Systems Administrator, other RioOne Health Officials as deemed necessary

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(7)(i), Contingency Plan [Standard; Required]

RioOne Health	HIPAA Security	Policy ID: HS-13
Title: **Data Backup Plan and Disaster Recovery Plan**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI."

"Establish (and implement as needed) procedures to restore any loss of data."

Purpose Statement: To the extent that RioOne Health maintains ePHI within the Network, RioOne Health will implement plans to create, maintain, and recover exact copies of such ePHI. The ability to recover exact copies of this ePHI will enable RioOne Health to restore or recover any loss of ePHI and to restore the Network after damage caused by an emergency or disaster, such as fire, vandalism, terrorism, system failure, or natural disaster.

Policy/Procedure:

1. RioOne Health's secure servers are housed at a Tier 3 data center. The Tier 3 data center lies on two power grids and is further supported by a backup generator. In addition, the data center network incorporates extensive redundancy to protect data in the event of an emergency. These backup safeguards reinforce RioOne Health's commitment to ensure continuous operations of its servers, which minimizes the likelihood that ePHI will be lost during an emergency or Contingency Event.
2. Despite the presence of redundant circuits that the data center provides for RioOne Health's servers to protect data exchanged through the Network, RioOne Health conduct weekly full backups with nightly backups of incremental data sets, and stores the backed-up data on a separate server.
3. The backup server is located at the data center, within the secured RioOne Health cabinet that houses the Network server.
4. RioOne Health will periodically test its Data Backup Plan to ensure that critical business processes can continue in a satisfactory manner during a disaster. If necessary, RioOne Health may revise the Data Backup Plan, and the occurrence of any of the following events may result in a revision of the Data Backup Plan:
    a. Changes to RioOne Health's physical or technical infrastructure or operating systems;
    b. Changes in threats to the Network; or
    c. Results of testing that indicate that the plan needs to be modified to ensure that it is sufficient, accurate, and up-to-date.
5. In the event of an emergency or disaster, such as a fire, vandalism, terrorism, system failure, or natural disaster, RioOne Health will use data retrieved from its backup server to restore Network functionality in accordance with the Contingency Plan Policy (HS-12) and the Data Backup and Disaster Recovery Plan Policy (HS-13).

Responsibility: Security Officer; Systems Administrator

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(7)(ii)(A), Data Backup Plan [Implementation Specification; Required]
- 45 C.F.R. §164.310(d)(2)(iv), Data backup and storage [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(7)(ii)(B), Disaster Recovery Plan [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(7)(ii)(D), Testing and Version Procedures [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-14
Title: **IT Security and Risk Management Plan**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode (IT Security and Risk Management Plan)."

Purpose Statement: RioOne Health will develop and implement an IT Security and Risk Management Plan to enable the continuation of its critical business processes and to protect the security of ePHI while RioOne Health operates in emergency mode. RioOne Health's IT Security and Risk Management Plan will permit authorized Users to access and use the Network during and immediately following an emergency or disaster. Emergency mode operation procedures detailed in the IT Security and Risk Management Plan must be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while RioOne Health operates in emergency mode.

Policy/Procedure:

1. RioOne Health's IT Security and Risk Management Plan will:
    a. Define and categorize reasonably foreseeable emergencies and/or disasters that could have an impact on the confidentiality, integrity, and availability of ePHI that is exchanged through the Network.
    b. Include a procedure that specifies how RioOne Health will react to emergencies and disasters.
    c. Include a procedure that outlines how RioOne Health will maintain security processes and controls during and immediately following an emergency or disaster.
    d. Authorize designated Workforce Members to enter RioOne Health's offices and facilities and any offsite location where backup media are stored to maintain the security process and controls of the Network.
    e. Identify the roles that particular RioOne Health Workforce Members will serve while RioOne Health is operating in emergency mode.
    f. Identify the roles of designated Workforce Members who will be permitted to administer or modify processes and controls that protect the security of ePHI while RioOne Health is operating in emergency mode.
2. RioOne Health will make its IT Security and Risk Management Plan easily available to its Workforce Members at all times.
3. RioOne Health will periodically test its IT Security and Risk Management Plan to ensure that critical business processes can continue in a satisfactory manner. If necessary, RioOne Health may revise the IT Security and Risk Management Plan, and the

occurrence of any of the following events may result in a revision of the IT Security and Risk Management Plan:

a. Disaster recovery role and responsibility changes, including changes to contact information.
b. Changes to RioOne Health's physical or technical infrastructure or operating systems.
c. Changes in threats to the Network.
d. Results of testing that indicate that the plan needs to be modified to ensure that it is sufficient, accurate, and up-to-date.

Responsibility: Security Officer; Systems Administrator

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(7)(ii)(C), Emergency Mode Operation Plan [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(7)(ii)(D), Testing and Version Procedures [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-15
Title: **Applications and Data Criticality Analysis**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Assess the relative criticality of specific applications and data in support of other contingency plan components."

Purpose Statement: The purpose of the criticality analysis is for RioOne Health to document the impact to its services, processes, and operating objectives if a disaster or other emergency causes any or all of the Network's functions to become unavailable for a documented period of time. The criticality analysis will serve as the basis for the prioritization of each Network function and the importance of the function to RioOne Health's business operations during a disaster.

Policy/Procedure:

1. To prioritize functions within the Network for disaster recovery, the Information Technology Department will develop a matrix, which:
    a. Inventories all the Network functions; and
    b. Determines the necessity of each Network function to RioOne Health's operations.
2. The matrix will be used to determine which of the Network functions are most important to the operation of RioOne Health's critical business operation and thereby determine how disaster recovery efforts will be focused during a Contingency Event or other disaster.
3. The matrix may direct:
    a. Which Network functions will be restored first; and/or
    b. Which Network functions will receive the first line of assistance during a disaster.
4. RioOne Health will conduct a yearly data criticality analysis as part of its risk assessment in accordance with the IT Security and Risk Management Plan, Evaluation and Updates Policy (HS-1).
5. The Systems Administrator will be responsible for documenting all activities relating to the data criticality analysis and providing such documentation to any Vendor that needs this information in connection with the IT Security and Risk Management Plan (HS-14). Such documentation will be maintained and retained by the Security Officer for six years from the date of creation.

Responsibility: Systems Administrator; Security Officer; Vendor

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(7)(ii)(E), Applications and Data Criticality Analysis [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-16
Title: **Facility Access and Security**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."

Purpose Statement: RioOne Health and its Vendor(s), to the extent applicable, will ensure that physical access to the servers that host the Network is limited.

Policy/Procedure:

FACILITY ACCESS AND SECURITY CONTROLS

1. The server that maintains all of the ePHI exchanged through the Network is housed in a Tier 3 data center. RioOne Health, in its discretion, may relocate its servers to another Tier 3 or higher data center.
2. All RioOne Health servers are contained within RioOne Health's designated, locked cage at the data center.
3. The data center is locked at all times, and only grants authorized personnel limited physical access through the use of biometric security measures. In addition, the following security controls are utilized in the data center to protect the facility, and RioOne Health's servers, from unauthorized access, tampering and theft:
    a. Signs and warnings stating that access to an area is restricted
    b. Surveillance cameras
    c. Alarms

RioOne Health, in its discretion, may evaluate, from time to time, the need for additional security controls to be put into place by its Vendors to protect the physical security of its servers.

4. Designated Workforce Members and/or Vendor personnel will personally supervise all visitors and vendors while they are physically present at the data center in the secured cabinet that houses the servers.

FACILITY REPAIRS AND MODIFICATIONS

1. The data center is responsible for conducting all necessary repairs and modifications to its facility to either repair or enhance its security features.
2. The data center will notify the Security Officer if any repairs or modifications are required for the cabinet containing RioOne Health's server and backup server. RioOne Health will document and maintain such notifications.

Responsibility: Security Officer; Vendor

Regulatory Category: Physical Safeguards

Regulatory Reference:

- 45 C.F.R. §164.310(a)(1), Facility Access Controls [Standard; Required]
- 45 C.F.R. §164.310(a)(2)(i), Contingency Operations [Implementation Specification; Addressable]
- 45 C.F.R. §164.310(a)(2)(ii), Facility Security Plan [Implementation Specification; Addressable]
- 45 C.F.R. §164.310(a)(2)(iii), Access Control and Validation Procedures [Implementation Specification; Addressable]
- 45 C.F.R. §164.310(a)(2)(iv), Maintenance Records [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-17
Title: **Workstation Use and Security**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI."

"Implement physical safeguards for workstations that access electronic PHI to restrict access to authorized users."

Purpose Statement: Workstations will be used in a manner that is consistent with RioOne Health's business purposes. RioOne Health requires the implementation of reasonable physical safeguards to protect all workstations and other electronic devices that access, store or transmit ePHI from theft or unauthorized use. RioOne Health will periodically review, and may modify, as appropriate, the permitted and prohibited uses of Workstations and the security controls implemented to protect Workstations in accordance with the IT Security and Risk Management, Evaluation and Updates Policy (HS-1). RioOne Health will periodically distribute training and education materials to Workforce Members regarding the use and security of Workstations used to access the Network.

Policy/Procedure:

WORKSTATION USE AND SECURITY FOR WORKFORCE MEMBERS

1. RioOne Health's Workstations will only be used for business purposes.
2. RioOne Health will locate Workstations in physically secure areas and will physically position Workstations in ways that minimize unauthorized viewing of ePHI.
3. Workstations will not be located in any of the following locations:
    a. Public walkways
    b. Hallways
    c. Waiting areas
    d. Any other area where unauthorized viewing of ePHI may occur
4. In the event that unauthorized viewing of ePHI cannot be minimized by positioning the Workstation, RioOne Health will install a screen filter on the Workstation.
5. RioOne Health will require Workforce Members to have unique user identifiers and passwords to gain access to their Workstations.
6. Workforce members must activate workstation locking software upon leaving a Workstation for more than five (5) minutes.
7. **Workforce members** must log-off from their Workstations when their work-day shift is complete.

8. RioOne Health will ensure that anti-virus software, which is configured to receive anti-virus updates, is installed on all Workstations that its Workforce Members use in accordance with the Malicious Software Policy (HS-9).
9 .These same Workstation security procedures apply to all Workstations regardless of the Workstation's location.
10. Portable Workstations must be physically secured at all times when not in the Workforce Member's immediate possession while such workstations are off-site.

Responsibility: Security Officer; Systems Administrator; Workforce Members

Regulatory Category: Physical Safeguards

Regulatory Reference:

- 45 C.F.R. §164.310(b), Workstation Use [Standard; Required]
- 45 C.F.R. §164.310(c), Workstation Security [Standard; Required]

RioOne Health	HIPAA Security	Policy ID: HS-18
Title: **Device and Media Controls**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility."

Purpose Statement: RioOne Health will take reasonable and appropriate steps to control its hardware and electronic media throughout the media's entire lifecycle, from initial receipt to final removal. Such control includes reasonably and appropriately protecting, accounting for, storing, backing up, and disposing of its hardware and electronic media in accordance with specific control procedures and tracking all incoming hardware and electronic media and transfers of hardware and electronic media as they are moved into and out of RioOne Health's direct control and premises.

Policy/Procedure:

INVENTORY AND MOVEMENT OF HARDWARE AND ELECTRONIC MEDIA

1. RioOne Health will periodically take an inventory of hardware and electronic media that contain ePHI. Workforce Members and RioOne Health Information Exchange or Health Direct Users will be advised that they should not save any ePHI to electronic media unless required to perform their job functions.
2. If a Workforce Member is required to save ePHI to electronic media to perform his job functions, it may only be saved to hard drives and approved USB drives. No other media may be used to store ePHI.
3. Prior to moving hardware or other electronic media that contain ePHI outside of RioOne Health's facilities and out of the direct control of RioOne Health, the Security Officer must be notified of and grant authorization for such movement.
4. RioOne Health will maintain documented records regarding the movement outside of RioOne Health's facilities and direct control of hardware and electronic media that contains ePHI. Documentation regarding the movement of hardware or electronic media will be required only for desktop computers, laptops, and other media storage devices that can be tracked. The following information must be documented in each record regarding the movement of hardware or electronic media:
    a. Date of movement
    b. Method of movement
    c. Description of the moved medium
    d. Dates indicating the time period that the moved medium was used at RioOne Health
    e. Dated signatures of the Security Officer and all Workforce Members supervising the movement.

DISPOSAL OF ePHI, HARDWARE AND ELECTRONIC MEDIA

See Sanitation Documents

1. Hardware and Electronic Media
    a. RioOne Health will take all reasonable and appropriate steps to remove ePHI from hardware and electronic media prior to the final disposal of the hardware or electronic media.
    b. The Security Officer or designee will determine which sanitization method is appropriate for the removal of ePHI from hardware and/or electronic media.
    c. The following sanitization methods may be used to remove ePHI from hardware and/or electronic media:
        i. Clearing
            1. Overwrites storage space on the hardware or electronic media with non-sensitive data.
            2. The hardware and/or electronic media type and size may influence whether overwriting is a suitable sanitization method.
            3. RioOne Health will consult the National Institute of Standards and Technology (NIST) *Guidelines for Media Sanitization*, Publication 800-88 regarding recommendations for clearing different media types.
        ii. Purging
            1. Degaussing is an acceptable method of purging.
            2. Degaussing exposes the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains.
            3. Degaussing cannot be used to purge nonmagnetic media, such as optical media or compact discs (CDs).
            4. RioOne Health will consult the National Institute of Standards and Technology (NIST) *Guidelines for Media Sanitization*, Publication 800-88 regarding its recommendations for purging different media types.

        iii. Disposing: If hardware and/or electronic media cannot be cleared or purged, the only method of disposal is to physically destroy the hardware and/or electronic media. Acceptable methods of destroying hardware and/or electronic media include:
            1. Disintegration
            2. Incineration
            3. Pulverization
            4. Melting
            5. Shredding
    d. RioOne Health will document the disposal of all hardware and electronic media disposal and the steps taken to remove ePHI prior to the disposal of such hardware and electronic media.
    e. The Security Officer or designee will inspect all hardware and

electronic media to ensure that all ePHI has been removed from the hardware or electronic media prior to disposal.

MEDIA RE-USE

1. For the internal re-use of hardware and/or electronic media, such as the re-deployment of a computer to another Workforce Member, RioOne Health will reformat all files on the hardware and/or electronic media so that such files are not accessible.
2. For external re-use of hardware and/or electronic media (e.g. donation or return of leased hardware), RioOne Health will completely and permanently remove ePHI from the hardware and/or electronic media in accordance with the Disposal procedures of this Policy.

Responsibility: Security Officer; Systems Administrator; Workforce Members

Regulatory Category: Physical Safeguards

Regulatory Reference:

- 45 C.F.R. §164.310(d)(1), Device and Media Controls [Standard; Required]
- 45 C.F.R. §164.310(d)(2)(i), Disposal [Implementation Specification; Required]
- 45 C.F.R. §164.310(d)(2)(ii), Media Re-Use [Implementation Specification; Required]
- 45 C.F.R. §164.310(d)(2)(iii), Maintenance of Records regarding Movements of Hardware and Media [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-19
Title: **Technical Access Controls**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F.R. §164.308(a)(4)."

45 C.F.R. §164.308(a)(4) states, "Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of subpart E of this part."

Purpose Statement: To protect the confidentiality, integrity, and availability of ePHI, RioOne Health has taken reasonable and appropriate steps to ensure that there are technical safeguards to control and restrict access to the Network to persons who are authorized to have such access in accordance with the Information Access Management Policy (HS-5).

Policy/Procedure:

RioOne Health will implement appropriate technical security controls and methods that permit only authorized persons to access the Network. Such controls and methods may include, but are not limited to, the following:

a. When appropriate, issuance of unique user identifications (user IDs) for each User to be used in conjunction with passwords and a second authentication method as part of RioOne Health's dual-factor authentication measures.
b. Emergency access procedures that enable authorized Workforce Members to obtain access to the Network during a disaster or other emergency.
c. Activation of password protected screensaver on internal Workstations after a designated period of inactivity.
d. Automatic log-off after a designated period of inactivity in accordance with the Log-In Monitoring and Automatic Log-Off Policy (HS-10).
e. Requiring Workforce Members to log-off or lock Workstations upon leaving their work areas.
f. Encryption, when appropriate, of ePHI exchanged through the Network.

EMERGENCY ACCESS PROCEDURE

RioOne Health may not need to access the Network during an emergency or disaster. However, if RioOne Health does require such access during an emergency or disaster, RioOne Health will follow the procedures outlined in its Contingency Plan Policy (HS-12) and IT Security and Risk Management Plan (HS-14) regarding who has access to the Network.

WORKSTATION SCREENSAVERS FOR RIOONE HEALTH WORKFORCE MEMBERS

1. All RioOne Health Workstations will be equipped with screensavers that will automatically activate after 5 minutes of inactivity.
2. Workforce Members can only deactivate the Workstation screensaver by entering his or her confidential password when prompted.

ENCRYPTION AND DECRYPTION

1. Based on its risk analysis in accordance with the IT Security and Risk Management, Evaluation and Updates (HS-1), RioOne Health will determine when to implement encryption for ePHI exchanged through the Network and the type and quality of the encryption algorithm and cryptographic key length for data that RioOne Health controls and maintains.
2. The Security Officer will approve the encryption mechanism that RioOne Health will use.
3. When encryption is used, RioOne Health will:
    a. Protect its cryptographic keys against modification and destruction, and protect its private keys against unauthorized disclosure.
    b. Manage the cryptographic keys used to encrypt ePHI exchanged through the Network.
    c. Periodically determine activation and deactivation dates for its cryptographic keys.

Responsibility: Security Officer; Systems Administrator; Vendors

Regulatory Category: Technical Safeguards

Regulatory Reference:

- 45 C.F.R. §164.312(a)(1), Access Control [Standard; Required]
- 45 C.F.R. §164.312(a)(a)(2)(i), Unique User Identification [Implementation Specification; Required]
- 45 C.F.R. §164.312(a)(2)(ii), Emergency Access Procedure [Implementation Specification; Required]
- 45 C.F.R. §164.312(a)(a)(2)(iii), Automatic Logoff [Implementation Specification; Addressable]
- 45 C.F.R. §164.312(a)(a)(2)(iv), Encryption and Decryption [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-20
Title: **Integrity**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement policies and procedures to protect electronic PHI from improper alteration or destruction."

Purpose Statement: To safeguard ePHI, it is important to ensure that ePHI has not been altered or destroyed in an unauthorized manner. Therefore, RioOne Health will take reasonable and appropriate steps to protect the integrity of ePHI exchanged through the Network.

Policy/Procedure:

1. Under no circumstances are Workforce Members permitted to modify or alter clinical information exchanged through the Network.
2. Except as set forth in this Policy or Deletion of RioOne Health Information Exchange or Health Direct Messages Policy (DM-13), ePHI exchanged through the Network will not be destroyed without first providing notice to and receiving authorization from the Security Officer in accordance with the Device and Media Controls Policy (HS-18).
3. RioOne Health has sufficient policies and procedures in place that minimize the need to authenticate ePHI; therefore, it is not reasonable or appropriate to implement additional mechanisms to authenticate ePHI.

Responsibility: Security Officer

Regulatory Category: Technical Safeguards

Regulatory Reference:

- 45 C.F.R. §164.310(c)(1), Integrity [Standard; Required]
- 45 C.F.R. §164.310(c)(2), Mechanisms to Authenticate Electronic PHI [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-21
Title: **Person or Entity Authentication**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed."

Purpose Statement: To protect the confidentiality, integrity, and availability of ePHI, RioOne Health will maintain a documented process for verifying the identity of any person or entity prior to granting access to the Network.

Policy/Procedure:

1. RioOne Health requires the use of at least dual-factor authentication before access to the Network is granted.
    a. User IDs are assigned in accordance with the Technical Access Controls Policy (HS-19).
    b. All passwords must be complex and confidential in accordance with the Password Management Policy (HS-11).
    c. A unique second method of authentication will be used each time the Network is accessed.
2. RioOne Health will not allow redundant authentication credentials.
3. When feasible, RioOne Health will mask, suppress, or otherwise obscure the passwords of persons and entities seeking access to the Network so that unauthorized persons are not able to observe such passwords.
4. RioOne Health will limit the authentication attempts of persons seeking access to the Network a five attempts at one time. Authentication attempts that exceed this limit may result in:
    a. Logging of the event for review;
    b. Disabling of the User's password; or
    c. Notifying the Security Officer or other appropriate RioOne Health official.
5. The credentials of each User will be verified pursuant to the Information Access Management Policy (HS-5).

Responsibility: Security Officer

Regulatory Category: Technical Safeguards

Regulatory Reference:

- 45 C.F.R. §164.312(d), Person or Entity Authentication [Standard; Required]

RioOne Health	HIPAA Security	Policy ID: HS-22
Title: **Transmission Security**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network."

Purpose Statement: To ensure the confidentiality, integrity, and availability of ePHI, RioOne Health will implement technical security measures to guard against unauthorized access to ePHI while it is transmitted over electronic communications networks.

Policy/Procedure:

1. RioOne Health will implement secure protocols, which encrypt data while such data is being electronically transmitted. In addition, these secure protocols allow decrypted data to be presented to the User upon its arrival to his or her Workstation.
2. Unauthorized access to ePHI transmitted through the Network is prevented through the use of the administrative, technical and physical safeguards for the Network described in the Policies and Procedures.

Responsibility: Security Officer; Systems Administrator

Regulatory Category: Technical Safeguards

Regulatory Reference:

- 45 C.F.R. §312(e)(1), Transmission Security [Standard; Required]
- 45 C.F.R. §312(e)(2)(i), Integrity Controls [Implementation Specification; Addressable]
- 45 C.F.R. §312(e)(2)(ii), Encryption During Transmission [Implementation Specification; Addressable]

RioOne Health	HIPAA Security	Policy ID: HS-23
Title: **Availability**	Version: 1	Effective Date: **Draft**

HIPAA Security Rule Language: "Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains."

Purpose Statement: RioOne Health will make all documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Policy/Procedure:

1. RioOne Health will make the following documentation available to those persons responsible for implementing these Policies and Procedures:
    a. Policies and procedures regarding the security of ePHI and the Network.
    b. All documentation that records any updates, revisions, modifications, or deletions made to existing Privacy and Security Policies and Procedures.
    c. All policies and procedures no longer in effect for a certain Security Regulation requirement or implementation specification.
    d. Any other documentation that the Security Officer deems appropriate to retain and to make available to Users regarding RioOne Health's Policies and Procedures.
2. The Security Officer will be responsible for ensuring that such documentation as required by the HIPAA Security Regulations is made available to Users.
3. All documentation specified in this policy will be available on the Network.

Responsibility: Security Officer

Regulatory Category: Policies, Procedures, and Documentation

Regulatory Reference:

- 45 C.F.R. §164.316(b)(2)(ii), Availability [Implementation Specification; Required]

RioOne Health	HIPAA Security	Policy ID: HS-24
Title: **Provision of Notice**	Version: 1	Effective Date: **Draft**

PURPOSE:
To provide individuals with adequate notice of the uses and disclosures of PHI that may be made by RioOne Health through the Exchange and of the individual's rights and RioOne Health legal duties with respect to PHI.

POLICY:
Provision of Notice
As required by Section 181.154 of the Health and Safety Code, RioOne Health will provide notice to individuals that their PHI is subject to electronic disclosure and explain how an HIE facilitates the exchange of data to promote individual's health. RioOne Health is a covered entity under state law as are Participants.

PROCEDURE:
1. RioOne Health will post the required notice on the RioOne Health website.
2. The notice will be reviewed annually with RioOne Health employees having access to PHI and all new employees during their orientation to RioOne Health.
3. A copy of any revisions to the notice will be distributed to all employees.
4. RioOne Health's Privacy Officer will keep a copy of the notice and revisions thereof for such period required by law.
5. Questions regarding the notice should be referred to the RioOne Health Privacy Officer.

Content of Notice
1. The notice contains descriptions of RioOne Health's role as a health information exchange in facilitating the exchange of information among Participants to improve access, quality and outcomes of care, and the fact that RioOne Health is not a direct provider of care.
2. The notice contains statements that RioOne Health:
   A. Maintains the privacy of PHI and provides individuals with notice of its legal duties and privacy practices with respect to PHI; and
   B. Abides by the terms of the Notice currently in effect.
3. The notice contains a statement that individuals may complain to RioOne Health if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with RioOne Health and a statement that the individual will not be retaliated against for filing a complaint.
4. The notice contains the name and telephone number of RioOne Health's Privacy Officer.

Responsibility: Security Officer

Regulatory Category: Policies, Procedures, and Documentation

Regulatory Reference: 45 CFR 164.502(i); 45 CFR 164.520(a)(b)(c)(e);Texas Health & Safety Code §181.54, Availability [Implementation Specification; Required]

RioOne Health	**HIPAA Security**	Policy ID: HS-25
Title: **Notification in the case of Breach of Unsecured Protected Health Information**	Version: 1	Effective Date: **Draft**

PURPOSE:
To establish a breach notification process applicable to Unsecured PHI.

APPLICABILITY:
This policy applies to RioOne Health and RioOne Health Business Associates, who access, maintain, retain, modify, record, store, destroy, or otherwise hold, use or disclose Unsecured PHI.

DEFINITIONS:

Breach: means the unauthorized acquisition, access, use or disclosure of Unsecured PHI, which compromises (i.e., poses a significant risk of financial, reputational, or other harm to the individual) the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Data Disposed: includes discarded paper records or recycled electronic media.

Data in Motion: includes data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange.

Data at Rest: includes data that resides in databases, file systems, flash drives, memory, and any other structured storage method.

Data in Use: includes data in the process of being created, retrieved, updated, or deleted.

Law Enforcement Official: means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, empowered by law to: (1) Investigate or conduct an official inquiry into a potential violation of law; (2) Prosecute or otherwise conduct an official inquiry into a potential violation of law; or (3) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Unsecured Protected Health Information: means PHI that is not secured through the use of a technology or methodology specified by the Secretary of HHS ("Secretary") guidance.

POLICY:

General Duty.
In the event RioOne Health discovers a breach of Unsecured PHI, RioOne Health will notify the Participant who provided RioOne Health the individual(s) PHI that has been, or is reasonably believed by RioOne Health to have been, inappropriately accessed, acquired, or disclosed as a result of such breach, as outlined below.

A breach shall be treated as discovered by RioOne Health or the Business Associate as of the first day on which such breach is known to, or by exercising reasonable diligence would have been known to, RioOne Health or the Business Associate as applicable.

The notification requirements of this Policy apply to breaches committed by RioOne Health Business Associates. Following discovery of a breach, Business Associates must notify RioOne Health of the breach and identify those individuals whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been breached.

Determination of a Breach.
In the event RioOne Health or the RioOne Health Business Associate discovers a breach, RioOne Health's Privacy Officer shall document:

1. the identification of each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during the Breach;
2. the date of the Breach, if known;
3. the scope of the Breach;
4. a description of RioOne Health or the Business Associate's response to the Breach; and
5. that notification of the breach was provided to the Participant or the reasons that RioOne Health determined that such notification was not necessary in accordance with step below.

PERFORMANCE OF RISK ASSESSMENT:
In order to determine whether a breach of PHI, requires that the Participant be informed, the Privacy Officer shall:

Step 1: ***Determine Whether a Breach of the HIPAA Privacy Rule Occurred.*** For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule.

Step 2: ***Determine whether the Improper Acquisition, Use or Disclosure Constitutes a "Breach" for Purposes of HITECH.*** Under HITECH, the term "breach" does not includes:

1. Unintentional acquisitions, access, or uses of PHI by an employee or individual acting under the authority of RioOne Health or the Business Associate of RioOne Health if:
   (a) The acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of a workforce member while working under the authority of RioOne Health or the RioOne Health Business Associate; and
   (b) The information is not further acquired, accessed, used, or disclosed by any person.
2. Inadvertent disclosures from an individual otherwise authorized to access PHI at the RioOne Health or RioOne Health Business Associate's office if:
   (a) The disclosure is to another similarly situated individual at the same office; and
   (b) The information is not further acquired, accessed, used or disclosed by any person without patient authorization.
3. A disclosure of PHI where RioOne Health or the RioOne Health Business Associate (upon conferring with RioOne Health's Privacy Officer) has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. RioOne Health's Privacy Officer should complete the analysis on Step 4 below in making this determination.
4. If information is de-identified in accordance with 45 C.F.R. §165.514, it is not PHI and thus any inadvertent or unauthorized disclosure of such information will not be considered a breach.

To the extent an acquisition, use or disclosure falls into one of the above four (4) categories; the Privacy Officer need not notify the Participant of the use or disclosure or continue with subsequent steps. However, the Privacy Officer should document the acquisition, use or disclosure in a RioOne Health Accounting Log in accordance with 45 C.F.R. §165.528.

Step 3: ***Determine the Nature of Data Elements Breached.*** A use or disclosure of PHI that does not include the following identifiers does not compromise the security or privacy of the PHI:

(a) Names;
(b) Postal address information, other than town or city, State;
(c) Telephone numbers;
(d) Fax numbers;
(e) E-mail addresses;
(f) Social security numbers;

(g) Medical record numbers;
(h) Health plan beneficiary numbers;
(i) Account numbers;
(j) Certificate/license plate numbers;
(k) Vehicle identifiers and serial numbers;
(l) Device identifiers and serial numbers;
(m) Web URLs;
(n) Internet Protocol (IP) address numbers;
(o) Biometric identifiers, including finger and voice prints;
(p) Full face photographic images and any comparable images;
(q) Date of birth; or
(r) Zip code.

A. To the extent that the use or disclosure does not involve the above identifiers, the Privacy Officer need not continue to Step 4 and notice to the Participant is not required. However, the Privacy Officer shall log the improper use or disclosure in a RioOne Health Accounting log. In addition, the Privacy Officer shall document in a Risk Assessment log that the use or disclosure of PHI did not include the above identifiers.

B. To the extent the use or disclosure of PHI includes the above referenced identifiers; the Privacy Officer shall perform the following steps of the risk assessment.

Step 4: ***Determine the Likelihood that the PHI is Accessible and Useable by Unauthorized Persons.*** PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.
   The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.
   (a) Valid encryption processes for data at rest are consistent with NIST Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices.3
   (b) Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800–52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800–77, Guide to IPsec VPNs; or 800–

113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140–2 validated.[1]

2. The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

(a) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

(b) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization,[2] such that the PHI cannot be retrieved.

To the extent PHI is rendered unusable, unreadable, or indecipherable by the above materials, it is not necessary to provide notice to the Participant.

4
5

Step 5: ***Review the physical, technical, and procedural safeguards employed by RioOne Health or the RioOne Health Business Associate (as applicable).*** The Privacy Officer should review, or request that Business Associate review, appropriate counter-measures, such as monitoring systems, for misuse of the PHI and patterns of suspicious behavior, that can be taken by RioOne Health or RioOne Health's vendor, as applicable.

Step 6: ***Mitigate Harm.*** Upon determining that an impermissible use or disclosure occurred, the Privacy Officer shall, or as applicable request that RioOne Health's vendor, take immediate steps to mitigate the impermissible risk or disclosure.

When possible, the Privacy Officer or Business Associate, as applicable, shall obtain the recipient's written satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. If such mitigating steps eliminate or reduce the risk of harm to the individual to less than a "significant risk," it is not necessary for the Privacy Officer to provide notice to the Participant. In such event, the inappropriate disclosure or use should be noted in RioOne Health's Accounting Log.

Step 8: *Documentation.* The Privacy Officer shall document RioOne Health's Risk Assessment process and conclusions. To the extent that the Privacy Officer determines that it is not necessary to provide notice to the Participant, the Privacy Officer's Risk Assessment must demonstrate the factors considered in determining that breach notification was not required.

DEADLINE FOR NOTICE:

[1] Available at http://www.csrc.nist.gov/.
[2] Available at http://www.csrc.nist.gov/.

Notification to the Participant of a breach of Unsecured PHI shall be made without unreasonably delay after discovery of the breach.

METHODS OF NOTICE:
The method of notice to the Participant shall be determined by the Notice provisions of the Business Associate Agreement with the Participant who provided the PHI.

DOCUMENTATION:
The Privacy Officer shall maintain an internal log of breaches and document the process and results of any Risk Assessment. The Privacy Officer shall retain such documentation and forms for at least six (6) years.

Responsibility: Security Officer

Regulatory Category: Policies, Procedures, and Documentation

Regulatory Reference: 45 CFR 164.400 to 164.414; CFR 164.142; Business and Commerce Code Sec. 521.002; Business and Commerce Code Sec. 521.053, as amended by HB 30

Operational Policies

And

Procedures for the Network

RioOne Health	Operational Policy	Policy ID: O-1
Title: **Policy and Procedures Amendment Process**	Version: 1	Effective Date: **Draft**

Purpose Statement: RioOne Health will continuously review, and as necessary, revise all of its Policies and Procedures so that they remain current with the latest developments in the rapidly evolving HIE environment. It might be necessary to revise Policies and Procedures to comply with changes to the HIPAA Regulations; to incorporate new technologies that protect the confidentiality, integrity and availability of ePHI; to address any threats to the privacy or security of PHI that RioOne Health may encounter in the future; or to reflect any new governance or operational practices that are established.

Policy/Procedure:

1. The RioOne Health Governing Body will approve all new, amended, or replaced RioOne Health Policies and Procedures and repeal any existing RioOne Health Policies and Procedures. However, any Governing Body member, RioOne Health Information Exchange Participant or RioOne Health Direct User may submit in writing to RioOne Health a request for the development of a new Policy and Procedure, or a request for the amendment or repeal of an existing Policy and Procedure. All such requests shall identify:
    i. the Policy and Procedure that is the subject of the requested change (if any),
    ii. the type of Policy and Procedure sought (if it is a request for a new Policy and Procedure),
    iii. a thorough description of why the request is necessary, and
    iv. an analysis of the expected impact of adopting the new Policy and Procedure or modifying/repealing an existing Policy and Procedure.
2. The Chairman of the Board will consider any requests that meet the submission criteria set forth within thirty (30) days of following receipt of such request.
    a. If, after considering the request, the Executive Director determines that the request does not have merit or lacks sufficient detail, the Executive Director will communicate this determination to the requestor.
    b. If after considering the request, the Chairman of the Board determines that the request has merit, the Chairman of the Board will forward the request to a subcommittee or to staff to review the request and make a recommendation for action to the Chairman of the Board.
3. If the Executive Director approves a recommendation of a subcommittee or staff to adoption of a new, amended, or replaced Policy and Procedure or repeal a Policy and Procedure, it will forward such recommendation to the Governing Body. The Governing Body will then vote on whether to approve the recommended Policy and Procedure. If it is approved, the Governing Body will determine the effective date of such Policy and Procedure.
4. RioOne Health will use its best efforts to provide notice of such new, amended, repealed or replaced Policies and Procedures to RioOne Health Information Exchange Participants and RioOne Health Direct Users prior to the effective date of any such changes.

5. Documentation recording any changes or modifications to the Privacy and Security Policies and Procedures will be maintained for at least six years.

Responsibility: Chairman of the Board, RioOne Health Governing Body, RioOne Health Information Exchange Participants and RioOne Health Direct Users

RioOne Health	Operational Policy	Policy ID: O-2
Title: **Subpoena Response**	Version: 1	Effective Date: **Draft**

Purpose Statement: It is important that RioOne Health be responsive to a subpoena request but not disclose ePHI in an inappropriate manner.

Policy/Procedure:

1. Immediately upon receipt of any subpoena, RioOne Health will forward said subpoena to its legal counsel.
2. RioOne Health will follow advice of legal counsel regarding a response to a subpoena.
3. If the subpoena is requesting the health information of a specific person or persons whose ePHI was exchanged using the Network, counsel should be advised that RioOne Health takes the position that it is not the custodian of medical records and, therefore, is not the proper party to respond to the subpoena.

Responsibility: RioOne Health

RioOne Health	Operational Policy	Policy ID: O-3
Title: **Telephone Policy**	Version: 1	Effective Date: **Draft**

PURPOSE:
To establish proper procedures to prevent Workforce members from improper use or disclosure of PHI by telephone.

POLICY:
1. Medical information regarding an individual should generally not be released by phone. If an individual is requesting disclosure, Workforce members may disclose information only if that Workforce member:

A. Knows the individual and can verify the individual's identity by their voice; or
B. Individual provides their personal identifier number; or
C. Workforce member calls the individual at the phone number(s) provided in the individual's record.

2. Workforce members shall not disclose PHI to third parties, without individual authorization, except as authorized by law.

A. All disclosures to third parties must be documented in the individual's record.
B. Disclosures made for purposes other than treatment, payment, or health care operations shall be documented in a "Disclosure Record."

APPROVAL: by Privacy Officer; must contain Signature, Date
[Office (capacity)]; must contain Signature, Date

RioOne Health

Operational Policies and Procedures

For

RioOne Health Direct Messaging

RioOne Health	HIPAA Operational Policy for RioOne Health Direct Messaging	Policy ID: DM-1
Title: **RioOne Health Direct User Information Confidentiality**	Version: 1	Effective Date: **Draft**

Purpose Statement: RioOne Health will protect the confidentiality of all RioOne Health Direct User Information.

Policy/Procedure:

1. RioOne Health will not use or share RioOne Health Direct User Information with any person except as set forth in this Policy.
2. RioOne Health may access all RioOne Health Direct User Information submitted to RioOne Health and allow third parties who are performing services for RioOne Health to use this information for the benefit of RioOne Health.
3. RioOne Health may use a RioOne Health Direct User's name, email address, physical address, or other data to communicate with the User and to populate a RioOne Health Direct User Directory.
4. RioOne Health may use the RioOne Health Direct User Directory to facilitate communication between:
    a. the RioOne Health Direct User and other RioOne Health Direct Users through RioOne Health Direct Messaging; and
    b. the RioOne Health Direct User and others who are permitted by RioOne Health to communicate with RioOne Health Direct Users through RioOne Health Direct Messaging.
5. RioOne Health Direct Users may only access their personal RioOne Health Direct User Information. They may not access another RioOne Health Direct User's Information except as available through the RioOne Health Direct User Directory.
6. RioOne Health does not maintain a list of user passwords after their initial set-up.

Responsibility: RioOne Health, RioOne Health Direct Users

RioOne Health	Operational Policy for RioOne Health Direct Messaging	Policy ID: DM-2
Title: **Certificate Validation**	Version: 1	Effective Date: **Draft**

Purpose Statement: To ensure that only authorized RioOne Health Direct Users are sending messages using RioOne Health Direct Messaging, RioOne Health will validate the certificate for each message.

Policy/Procedure:

1. For each message that a RioOne Health Direct User sends using RioOne Health Direct Messaging, RioOne Health will check the validity of the certificate by verifying that
    a. The certificate has not expired;
    b. The message has a valid signature;
    c. The certificate has not been revoked;
    d. The certificate is binding to the expected entity; and
    e. The certificate has a trusted certificate path.

Responsibility: RioOne Health

RioOne Health	**Operational Policy for RioOne Health Direct Messaging**	Policy ID: DM-3
Title: **Direct Addresses**	Version: 1	Effective Date: **Draft**

Purpose Statement: To send and receive messages using RioOne Health Direct Messaging, each RioOne Health Direct User will be issued a unique RioOne Health Direct Messaging address.

Policy/Procedure:

1. Once an individual has successfully enrolled and been accepted as a RioOne Health Direct User pursuant to the RioOne Health Direct Messaging User Enrollment Policy (DM-8), they will be assigned a RioOne Health Direct Messaging address.
2. A RioOne Health Direct Messaging address will be structured as follows: firstname.lastname@direct.RioOneHealth.org.
3. A RioOne Health Direct User may share their RioOne Health Direct Messaging address with any other RioOne Health Direct User with whom they would like to exchange messages.
4. RioOne Health may list each RioOne Health Direct User's RioOne Health Direct Messaging address in a directory in accordance with the RioOne Health Direct User Information Confidentiality Policy (DM-1).

Responsibility: RioOne Health; RioOne Health Direct Messaging User

RioOne Health	**Operational Policy for RioOne Health Direct Messaging**	Policy ID: DM-4
Title: **Trusted HISPs**	Version: 1	Effective Date: **Draft**

Purpose Statement: RioOne Health only allows RioOne Health Direct Users to send messages to and receive messages from individuals who exchange such messages through a trusted health information service provider (HISP). This policy will set forth the procedure that RioOne Health uses to determine whether a HISP is trusted and a list of trusted HISPs.

Policy/Procedure:

1. During the first half of 2013, RioOne Health will develop a process by which it determines whether to admit a HISP into its circle of trust.
2. Until such a process is developed and RioOne Health expands its circle of trust to include other HISPs, RioOne Health Direct Users may only send messages to and receive messages from other RioOne Health Direct Users.

Responsibility: RioOne Health; RioOne Health Direct Users

RioOne Health	**Operational Policy for RioOne Health Direct Messaging**	Policy ID: DM-5
Title: **Agreements with RioOne Health Direct Users**	Version: 1	Effective Date: **Draft**

Purpose Statement: Each RioOne Health Direct User must agree to be legally obligated to protect the privacy, security and integrity of the information exchanged through RioOne Health Direct Messaging. Furthermore, RioOne Health must agree to be legally obligated to fulfill its responsibilities as a Business Associate of each RioOne Health Direct User. Each party's legal obligations are set forth in the RioOne Health Direct Messaging End User License Agreement and Business Associate Addendum.

Policy/Procedure:

1. All individuals that act as RioOne Health Direct Users must agree to the RioOne Health Direct Messaging End User License Agreement before the individual can access or use RioOne Health Direct Messaging.
2. Each RioOne Health Direct User, if it is a Covered Entity, must also enter into a Business Associate Agreement with RioOne Health where the User is the Covered Entity and RioOne Health is the Business Associate. The Business Associate Agreement is an addendum to the RioOne Health Direct Messaging End User License Agreement.

Responsibility: RioOne Health; RioOne Health Direct Users

RioOne Health	**Operational Policy for RioOne Health Direct Messaging**	Policy ID: DM-6
Title: **RioOne Health Use and Disclosure of PHI in RioOne Direct Messaging**	Version: 1	Effective Date: **Draft**

Purpose Statement: Pursuant to the RioOne Health Direct Messaging End User License Agreement, RioOne Health Direct Users are permitted to use RioOne Health Direct Messaging to send PHI to other RioOne Health Direct Users for any purpose allowed by law. RioOne Health, on behalf of the RioOne Health Direct User sending the message, delivers the information to the receiving RioOne Health Direct User. Pursuant to the Business Associate Agreement between RioOne Health and each RioOne Health Direct User, RioOne Health may also use and disclose PHI, as needed, for its proper management and administration and to fulfill any other obligations described in the RioOne Health Direct Messaging End User License Agreement.

Policy/Procedure:

1. RioOne Health may only use information provided by a RioOne Health Direct User, as needed, to perform certain proper management and administrative functions and fulfill its obligations under the RioOne Health Direct Messaging End User License Agreement. This includes, but is not limited to, encrypting messages sent by a RioOne Health Direct User, delivering messages to the RioOne Health Direct User recipient identified by the sending RioOne Health Direct User, and auditing and monitoring use of RioOne Health Direct Messaging as described in the RioOne Health Direct Messaging Auditing and Monitoring Policy (DM-7).
2. Each RioOne Health Direct User is responsible for making sure that all information he sends through RioOne Health Direct Messaging complies with applicable law. This includes obtaining any consents or authorizations required by applicable law prior to sending such information.

Responsibility: RioOne Health; RioOne Health Direct Users

RioOne Health	**HIPAA Operational Policy for RioOne Health Direct Messaging**	Policy ID: DM-7
Title: **RioOne Direct Messaging Auditing and Monitoring**	Version: 1	Effective Date: **Draft**

Purpose Statement: In accordance with the Information System Activity Review Policy (HS-2), RioOne Health will implement auditing and monitoring mechanisms to record and examine the activity of RioOne Health Direct Users in RioOne Health Direct Messaging to enable RioOne Health to detect potentially problematic activity.

Policy/Procedure:

AUDIT REPORT CONTENT

1. RioOne Health will create monthly audit reports that capture RioOne Health Direct User-level data associated with at least the following activities:
    a. User sign-ons to the RioOne Health Direct Messaging Service;
    b. Messages sent by a RioOne Health Direct User using RioOne Health Direct Messaging; and
    c. Failed authentication attempts after five (5) unsuccessful attempts to log-in to the RioOne Health Direct Messaging Service.
2. The monthly audit reports may generate the following information for each activity logged:
    a. Date and time of activity;
    b. Descriptions of each attempted or completed activity;
    c. Identification of the RioOne Health Direct User performing the activity; and/or
    d. Origin of the activity, such as the I/P address or workstation identification number.

RIOONE HEALTH DIRECT USER REQUESTS FOR AUDIT REPORTS

1. If a RioOne Health Direct User desires an audit report of their activity within RioOne Health Direct Messaging, they will submit a request to RioOne Health with a brief explanation of the reason for the request.
2. Within one week of receiving the request from the RioOne Health Direct User, RioOne Health will decide whether to accept or deny the request and transmit such decision to the RioOne Health Direct User.
3. If RioOne Health denies a request, RioOne Health will provide a brief explanation of the denial.
4. If RioOne Health accepts the request, RioOne Health will provide the RioOne Health Direct User with the requested report as soon as feasible.

Responsibility: RioOne Health, RioOne Health Direct Users

RioOne Health	**Operational Policy RioOne Health Direct Messaging**	Policy ID: DM-8
Title: **RioOne Direct Messaging User Enrollment**	Version: 1	Effective Date: **Draft**

Purpose Statement: To protect the confidentiality, integrity, and availability of ePHI exchanged through RioOne Health Direct Messaging, RioOne Health has implemented a strict enrollment process to ensure that only healthcare professionals who are regulated by the Texas Department of Health Professions have access to RioOne Health Direct Messaging.

Policy/Procedure:

1. Each individual who desires to use RioOne Health Direct Messaging will be responsible for completing the enrollment process.
2. To enroll, an individual must complete and submit the enrollment form. The enrollment form will require the individual to attest to the following:
   a. they have completely and accurately represented their identity,
   b. they are a healthcare provider with a valid license, certificate or registration issued by the Texas Department of Health Professions to practice their clinical occupation, and
   c. that such license, certificate or registration is currently in effect and in good standing.
3. The enrollment form must be notarized, scanned and submitted to RioOne Health at c.stewart@dhr-rgv.com (Subject line: enroll@RioOneHealth) or submitted via US Mail to RioOne Health Enrollment, 5501 S. McColl Rd, Edinburg, TX 78539.
4. The RioOne Health Direct User is responsible for maintaining accurate enrollment information and notifying RioOne Health of changes to such information so long as the individual remains a RioOne Health Direct User.
5. Beginning on the effective date, the individual must also send to RioOne Health at RioOne Health Enrollment, 5501 S. McColl Rd, Edinburg, TX 78539 a check made out to RioOne Health in the amount of the annual membership fee.
6. Once the individual submits all required enrollment information to RioOne Health, RioOne Health will verify with the Texas Department of Health Professions the status of the individual's professional license, certificate or registration.
7. Once RioOne Health has verified the status of the individual's professional license, certificate or registration and confirmed that it is in effect and in good standing, they will be assigned a unique username and temporary password to activate the User's access to RioOne Health Direct Messaging through the RioOne Health Direct Messaging Service. The first time the User signs-on to the RioOne Health Direct Messaging Service, they will be required to accept the RioOne Health Direct Messaging End User License Agreement. Once the User accepts the RioOne Health Direct Messaging End User License Agreement, they will change their password in accordance with the Password Management Policy (HS-11). The individual will then be able to send and receive messages through RioOne Health Direct Messaging.
8. RioOne Health will regularly confirm that each RioOne Health Direct User has a valid license, certificate or registration by checking each RioOne Health Direct User's license,

certificate or registration against reports of suspended or terminated licenses, certificates and registrations issued by the Texas Department of Health Professions.

9. If RioOne Health discovers that a RioOne Health Direct User's professional license, certificate or registration has been suspended or terminated, RioOne Health will suspend or terminate such User in accordance with the RioOne Health Direct User Suspension and Termination Policy (DM-9).

Responsibility: RioOne Health; RioOne Health Direct User

RioOne Health	**Operational Policy for RioOne Health Direct Messaging and HIE**	Policy ID: DM-9
Title: **RioOne Health Direct User Suspension and Termination**	Version: 1	Effective Date: **Draft**

Purpose Statement: RioOne Health will suspend or terminate a RioOne Health Direct User's access to RioOne Health Direct Messaging for the reasons set forth in the RioOne Health Direct Messaging End User License Agreement.

Policy/Procedure:

SUSPENSION PROCEDURES FOR RIOONE HEALTH DIRECT USERS

1. In accordance with the RioOne Health Direct Messaging and HIE End User License Agreement, RioOne Health can suspend a RioOne Health Direct User under the following circumstances:
   a. the RioOne Health Direct User's license, certificate or registration to practice their healthcare profession in the State of Texas is suspended;
   b. the RioOne Health Direct User violates any provision of the RioOne Health Direct Messaging and HIE End User License Agreement or any RioOne Health Policy and Procedure;
   c. the RioOne Health Direct User fails to pay their membership fee within sixty days of the date of the invoice; or
   d. upon discovering any material error or omission in the information that the RioOne Health Direct User provided during the Enrollment process.
2. To suspend a RioOne Health Direct User, RioOne Health will de-activate the id and password that the RioOne Health Direct User uses to access the RioOne Health Direct Messaging and HIE Service.
3. RioOne Health will provide notice of the suspension to the suspended RioOne Health Direct User as soon as possible. Such notice will contain an explanation of the reason(s) that the RioOne Health Direct User was suspended.
4. The RioOne Health Direct User will have ten (10) business days in which to respond to the notice of suspension by providing RioOne Health with a plan of correction to address the reason(s) for the suspension.
   a. If the RioOne Health Direct User fails to provide RioOne Health with a plan of correction, RioOne Health will terminate the RioOne Health Direct User.
   b. If the RioOne Health Direct User provided RioOne Health with a plan of correction, RioOne Health will have ten (10) business days in which to notify the RioOne Health Direct User whether the plan of correction is acceptable. If the plan of correction is not acceptable, then RioOne Health will inform the RioOne Health Direct User of the defects in the plan.

5. If, in RioOne Health's opinion, the reason(s) leading to the suspension of the RioOne Health Direct User is addressed, RioOne Health will re-activate the id of the RioOne Health Direct User and issue such User a new, temporary password. The RioOne Health Direct User will then use the temporary password to access to the RioOne Health Direct Messaging and HIE Service and change his password in accordance with the Password Management Policy (HS-11).

TERMINATION PROCEDURES FOR RIOONE HEALTH DIRECT USERS

1. In accordance with the RioOne Health Direct Messaging and HIE End User License Agreement, RioOne Health can terminate a RioOne Health Direct User under the following circumstances:
    a. the RioOne Health Direct User's license, certificate or registration to practice their healthcare profession in the State of Texas is revoked or otherwise terminated;
    b. the RioOne Health Direct User violates any provision of the RioOne Health Direct Messaging and HIE End User License Agreement or any RioOne Health Policy and Procedure and the violation is so serious that suspension is not an appropriate response;
    c. upon discovering any material error or omission in the information that the RioOne Health Direct User provided during the Enrollment process that is so serious that suspension is not an appropriate response;
    d. the RioOne Health Direct User fails to pay their membership fee within ninety days of the date of the invoice; or
    e. the RioOne Health Direct User has, in the opinion of RioOne Health, failed to adequately address the reason(s) leading to a suspension of the RioOne Health Direct User in accordance with the RioOne Health Direct Messaging and HIE End User License Agreement and this Policy.
2. To terminate a RioOne Health Direct User, RioOne Health will:
    a. De-activate the id and password that the RioOne Health Direct User uses to access the RioOne Health Direct Messaging and HIE Service; and
    b. Revoke the certificate issued to the RioOne Health Direct User.
3. RioOne Health will provide notice of termination to a terminated RioOne Health Direct User as soon as possible.

Responsibility: RioOne Health; RioOne Health Direct Users

RioOne Health	**Operational Policy for RioOne Health Direct Messaging and HIE**	Policy ID: DM-10
Title: **RioOne Health Direct Messaging and HIE Training**	Version: 1	Effective Date: **Draft**

Purpose Statement: RioOne Health will provide training information for RioOne Health Direct Users to optimize each RioOne Health Direct User's use of RioOne Health Direct Messaging and HIE and to help ensure that such Users will safeguard ePHI exchanged through RioOne Health Direct Messaging and HIE.

Policy/Procedure:

1. RioOne Health will provide training information to RioOne Health Direct Users that will teach them how to use the RioOne Health Direct Messaging and HIE Service.
2. As part of the training information, RioOne Health will provide information regarding methods to protect the confidentiality and integrity of ePHI.
3. RioOne Health may provide additional training from time to time as necessary.

Responsibility: RioOne Health

RioOne Health	**Operational Policy for RioOne Health Direct Messaging and HIE**	Policy ID: DM-11
Title: **RioOne Health Direct Messaging and HIE Service Log-In and Log-Off**	Version: 1	Effective Date: **Draft**

Purpose Statement: To regularly track the identification and authentication of those accessing RioOne Health Direct Messaging and HIE**,** RioOne Health will monitor log-in attempts to the RioOne Health Direct Messaging and HIE Service. RioOne Health will also enhance the security of RioOne Health Direct Messaging and HIE by automatically logging-off inactive RioOne Health Direct Users from the RioOne Health Direct Messaging and HIE Service.

Policy/Procedure:

UNIQUE USER IDS

1. RioOne Health will control access to RioOne Health Direct Messaging and HIE by assigning each RioOne Health Direct User who is granted access to RioOne Health Direct Messaging and HIE a unique user ID that:
   a. Identifies the individual; and
   b. Permits activities performed on RioOne Health Direct Messaging and HIE to be traced to the individual.
2. User IDs may consist of, but are not limited to:
   a. RioOne Health Direct User's name
   b. An identification number
   c. Biometric identification

LOG-IN PROCEDURES

1. A RioOne Health Direct User may only access the RioOne Health Direct Messaging and HIE Service after successfully entering their user id, password and second method of authentication. This process allows RioOne Health to verify the identity the RioOne Health Direct User.
2. After five consecutive, unsuccessful attempts to log-on to the RioOne Health Direct Messaging and/or HIE Service, the RioOne Health Direct User's password will be disabled. All such events will be logged as part of the monthly activity report pursuant to the RioOne Health Direct Messaging and HIE Auditing and Monitoring Policy (DM-7).
3. If a RioOne Health Direct User's password is disabled due to unsuccessful log-on attempts, the RioOne Health Direct User should contact the Systems Administrator.
4. The Systems Administrator will verify the RioOne Health Direct User's identity and determine whether the RioOne Health Direct User's access to the RioOne Health Direct Messaging and HIE Service was disabled because of five consecutive, unsuccessful attempts to log-on or by RioOne Health for another reason.

5. After verifying the RioOne Health Direct User's identity and that such User's access was disabled because of unsuccessful log-on attempts, the Systems Administrator will issue the RioOne Health Direct User a new, temporary password. The RioOne Health Direct

User will then use the temporary password to log-on to the RioOne Health Direct Messaging and HIE Service and re-set his or her own individual password in accordance with the Password Management Policy (HS-11).

AUTOMATIC LOG-OFF

1. A RioOne Health Direct User will be automatically logged-off of the RioOne Health Direct Messaging and HIE Service after 15 minutes of inactivity.
2. To activate a new session, a RioOne Health Direct User will have to log-on to the RioOne Health Direct Messaging and HIE Service using his or her user name, password and second method of authentication.

Responsibility: Security Officer; RioOne Health Direct User; Systems Administrator

RioOne Health	**Operational Policy for RioOne Health Direct Messaging and HIE**	Policy ID: DM-12
Title: **RioOne Direct Messaging and HIE Password Management**	Version: 1	Effective Date: **Draft**

Purpose Statement: To prevent unauthorized access to and use of RioOne Health Direct Messaging and HIE, RioOne Health requires RioOne Health Direct Users to take appropriate measures to select and secure passwords that allow such access to RioOne Health Direct Messaging and HIE.

Policy/Procedure:

1. All RioOne Health Direct Users will be given a user name, password and second method of authentication that allow them to access the RioOne Health Direct Messaging and HIE Service.
2. When a RioOne Health Direct User or Workforce Member logs-on to the RioOne Health Direct Messaging and HIE Service for the first time, they will be prompted to change the initial, temporary password provided to them by RioOne Health.
3. All passwords must comply with the Password Management Policy (HS-11).

Responsibility: RioOne Health Direct Users

RioOne Health	Operational Policy for RioOne Health Direct Messaging and HIE	Policy ID: DM-13
Title: **Deletion of RioOne Health Direct Messages**	Version: 1	Effective Date: **Draft**

Purpose Statement: RioOne Health allows RioOne Health Direct Users to retain messages that they receive through RioOne Health Direct Messaging and HIE in the RioOne Health Direct Messaging and HIE Service. For proper system administration and management, RioOne Health will periodically delete such messages in accordance with this Policy.

Policy/Procedure:

1. RioOne Health will allow RioOne Health Direct Users to retain messages received through RioOne Health Direct Messaging and HIE in the RioOne Health Direct Messaging and HIE Service.
2. A RioOne Health Direct User will be able to delete a message that they have received in the RioOne Health Direct Messaging and HIE Service. RioOne Health Direct Users are encouraged to delete messages after the message has been read and either printed or downloaded for the User's records.
3. RioOne Health will automatically delete messages from the RioOne Health Direct Messaging and HIE Service if the receiving RioOne Health Direct User has read the message and the message is more than 90 days old.
4. RioOne Health will monitor the number and size of messages retained by each RioOne Health Direct User in the RioOne Health Direct Messaging and HIE Service. If RioOne Health finds that the number or size of messages retained in the RioOne Health Direct Messaging and HIE Service by a RioOne Health Direct User are excessive, RioOne Health will contact such User to request that they delete their messages.

Responsibility: RioOne Health; RioOne Health Direct User

RioOne Health	Operational Policy for RioOne Health Direct Messaging and HIE	Policy ID: DM-14
Title: **RioOne Direct Messaging and HIE Encryption and Decryption**	Version: 1	Effective Date: **Draft**

Purpose Statement: To ensure the confidentiality, integrity, and availability of ePHI, RioOne Health will implement technical security measures, including encryption, to guard against unauthorized access to ePHI while it is transmitted through RioOne Health Direct Messaging and HIE.

Policy/Procedure:

ENCRYPTION AND DECRYPTION

1. RioOne Health will encrypt the content of all messages sent by a RioOne Health Direct User through RioOne Health Direct Messaging and HIE.
2. The content of the message will be encrypted using industry standard message encryption mechanisms and Secure Socket Layer (SSL) communications.
3. The header information in a message will not be encrypted. RioOne Health Direct Users are responsible for ensuring that PHI is not contained within the header.
4. RioOne Health will decrypt the content of the message for the RioOne Health Direct User receiving the message.
5. RioOne Health and its Vendor(s), to the extent applicable, will:
    a. Protect its cryptographic keys against modification and destruction, and protect its private keys against unauthorized disclosure.
    b. Manage the cryptographic keys used to encrypt ePHI exchanged through RioOne Health Direct Messaging and HIE.
    c. Periodically determine activation and deactivation dates for its cryptographic keys.

Responsibility: RioOne Health; RioOne Health Direct Users; Vendors