POLK COUNTY, IOWA
SECURITY POLICIES

FOR

COMPLIANCE WITH THE

HEALTH INSURANCE PORTABILITY

AND ACCOUNTABILITY ACT OF 1996

"HIPAA"

TABLE OF CONTENTS

Page(s)

HIPAA SECURITY POLICIES

GENERAL SECURITY COMPLIANCE

Polk County is committed to conducting business in compliance with all applicable laws, regulations and Polk County policies. Polk County has adopted this policy to set forth its compliance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the security of Electronic PHI ("ePHI") (the "Security Regulations").

This Policy covers Polk County's approach to compliance with the Security Regulations. As a covered entity under the Security Regulations, Polk County must:

(1) Ensure the confidentiality, integrity and availability of all ePHI Polk County 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 or required; and

(4) Ensure compliance with the Security Regulations by its Workforce.

Compliance with the Security Regulations will require Polk County to implement:

Administrative Safeguards--those actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect ePHI and to manage the conduct of Polk County's Workforce in relation to the protection of and authorized access to said ePHI.

Physical Safeguards--those physical measures, policies and procedures to protect Polk County's electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Technical Safeguards--the technologies and the policies and procedures for its use that protect ePHI and control access to it.

The Security Regulations permit Polk County to implement any security measure that allows it to reasonably and appropriately comply with a specific security standard in the Security Regulations. In determining which security measures to implement, Polk County has taken into account its size, complexity and capabilities; technical infrastructure; hardware and software security capabilities; the costs of the security measures; and the probability and criticality of potential risks to ePHI. Polk County has divisions, departments or subgroups who have different uses of PHI for Polk County. These groups will be referred to in this Security Manual as "Departments". In the Security Policies, Polk County has determined that Departments in some cases must implement a particular security measure and in other cases have discretion to determine which security measures to implement. In those cases in which a Security Policy permits a Department to exercise discretion in the implementation of a security measure, the Department

must notify and obtain the prior approval of the Security Officer for the measure implemented so that Polk County may ensure that it complies with the Security Regulations.

ASSIGNED SECURITY RESPONSIBILITY POLICY

I. POLICY

On behalf of its covered entity component parts, Polk County has designated a Security Officer with overall responsibility for the development and implementation of policies that conform to the Security Regulations, and to provide strategic direction and tactical management to ensure the security, confidentiality, availability, and integrity of ePHI.

Polk County's HIPAA Security Officer is Information Technology Director, currently Tony Jefferson.

II. PURPOSE

The purpose of this policy is to establish the duties and responsibilities of the Security Officer and each of the Department HIPAA Security Liaisons.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.308(a)(2)

IV. DUTIES OF SECURITY OFFICER

1) The Security Officer shall oversee the development, implementation and operation of Polk County's HIPAA Security Program. The Security Officer and/or each Department HIPAA Security Liaison shall have the following responsibilities:

   a) Develop and revise as needed these HIPAA Security Policies and Procedures and other mechanisms as necessary to address identified security threats and vulnerabilities to the confidentiality, integrity and availability of ePHI;
   b) Answer all questions from employees concerning the ePHI security safeguards, policies and procedures that are not adequately addressed by immediate supervision;
   c) Prepare cost benefit analyses of appropriate ePHI safeguards and make recommendations to management regarding the adoption of safeguards;
   d) Prepare the annual budgets for ePHI security;
   e) Meet with appropriate Individuals, including senior executives, the Privacy Officer and the Compliance Officer periodically, to discuss ePHI security issues, policies and planning;
   f) Ensure that all ePHI security policy and procedure manuals and materials are kept up to date and current with government rules, regulations and practices;
   g) Monitor Polk County's compliance with applicable ePHI security laws and regulations; monitor compliance with these HIPAA Security Policies and Procedures among Polk County employees and other third parties, and refer issues to appropriate managers or administrators;

h) Maintain records of access authorizations and document and review the levels of access granted to a user, program, or procedure accessing ePHI on an ongoing basis;

i) Develop appropriate ePHI security training program for Polk County employees;

j) Prepare and periodically assess Polk County's security incident response procedures, disaster recovery plan and business continuity plan for information systems containing ePHI;

k) Perform security audits and risk assessments of ongoing system activities utilizing ePHI;

l) Provide consulting support and make recommendations to management regarding appropriate, timely and necessary improvements or enhancements to the ePHI security program;

m) Coordinate ongoing review of existing ePHI security programs and initiate the development of new programs, as needed;

n) Investigate ePHI system security breaches, and, in consultation with the Privacy Officer and the Compliance Officer (or their designees), and administer appropriate sanctions related to security violations; and

o) Facilitate a process for Individuals to file a complaint regarding Polk County's Security Policies or the handling of ePHI by a Polk County HIPAA health care component, including ensuring that the complaint and its disposition are appropriately documented and handled.

2) Department HIPAA Security Liaisons. Each Department shall name a HIPAA Security Liaison. The Department HIPAA Security Liaison is responsible for assisting the HIPAA Security Officer in ensuring that the Department:

a) Complies with the HIPAA Security Policies

b) Develops and implements department specific HIPAA Security Procedures for each Security Policy that is applicable to that department,

c) Maintains the confidentiality of all ePHI created or received by the department from the date such information is created or received until it is destroyed, and

d) Trains all Workforce members within the Department at the appropriate level of HIPAA training as determined by the HIPAA Security Officer.

RISK ANALYSIS POLICY

I. POLICY

Polk County acknowledges the potential vulnerabilities associated with storing ePHI, transmitting ePHI locally, transmitting ePHI outside of Polk County, and transmitting ePHI to Polk County components that are not health care component parts. The Covered Enmity will identify and assess the system's vulnerabilities and any threats to the confidentiality, integrity, and availability of the ePHI on a periodic basis.

II. PURPOSE

The purpose of this policy is to establish guidelines for the periodic and accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI Polk County maintains.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.308(a)(1)(ii)(A)

IV. DUTIES OF SECURITY OFFICER AS TO RISK ANALYSIS

1) The Security Officer and each Department HIPAA Security Liaison shall:

   a) Identify and document all ePHI repositories, including present security controls or features in each repository
   b) Periodically re-inventory ePHI repositories
   c) Identify the potential vulnerabilities to each ePHI repository,
   d) Assess the probability that the vulnerability would be exploited;
   e) Assign a level of risk to each ePHI repository
   f) Determine risk mitigation strategies and appropriate mechanisms, safeguards, and controls
   g) Document the process; and
   h) Document the results.

2) Each Department HIPAA Security Liaison shall assist the Security Officer in reassessing the potential risks and vulnerabilities to the integrity, confidentiality, and availability of each ePHI repository and the level of risk assigned to each ePHI repository as needed.

3) ePHI repositories that otherwise would fall in the low or medium risk categories may be classified as high risk ePHI if the sensitivity or criticality of that information makes it appropriate to do so in the reasonable judgment of the Department HIPAA Security Liaison and the HIPAA Security Officer.

RISK MANAGEMENT POLICY

I. POLICY

Polk County will select and implement appropriate, cost-effective safeguards and will institute corrective action as necessary to protect the confidentiality, integrity, and availability of ePHI.

II. PURPOSE

The purpose of this policy is to ensure that Polk County implements security measures that are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.308(a)(1)(ii)(B)

SANCTION POLICY

I. POLICY

Polk County shall enforce appropriate discipline and sanction employees and other Workforce members for any violation of Security Policies and Procedures.

II. PURPOSE

The purpose of this policy is to notify Workforce members that Polk County will undertake disciplinary action against any Workforce member who violates these HIPAA Security Policies and Procedures.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(1)(ii)(C)
- Sanction Policy (Privacy Policies)

IV. SPECIFIC SANCTION POLICIES

1) To ensure that all users of Polk County's systems fully comply with these HIPAA Security Policies and Procedures, Polk County, will discipline and sanction such users, as appropriate, for any violation of the HIPAA Security Policies and Procedures.

2) Sanctions will be applied according to Polk County's Sanction Policy as set forth in Polk County's Privacy Policy, attached hereto and incorporated herein.

INFORMATION SYSTEM ACTIVITY REVIEW POLICY

I. POLICY

Polk County will collect and review data generated by system activity and will implement additional security safeguards or corrective action when necessary.

II. PURPOSE

The purpose of this policy is to monitor system activity through the periodic review of activity and records including audit logs, access reports, and security incident tracker reports.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(1)(ii)(D)
- Risk Management Policy
- Incident Procedures Policy

AUTHORIZATION AND/OR SUPERVISION POLICY

I. POLICY

Polk County will authorize Polk County employees whose job function requires the use of ePHI to have access to ePHI.

II. PURPOSE

The purpose of this policy is to ensure that appropriate Individuals are authorized to have access to ePHI.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(3)(ii)(A)
- HIPAA Workforce Clearance Policy
- Facility Access Control Policy
- Access Control Policy

IV. TO WHOM ACCESS TO ePHI SHALL BE AUTHORIZED

1) Polk County will authorize access to ePHI to those employees who require such access in order to perform his or her job.

   a) Polk County will review such access authorizations as appropriate.
   b) Access authorizations shall be revoked upon termination of employment or when access to ePHI is no longer necessary.

2) Whenever Polk County engages another person or entity (other than an officer, director or employee of Polk County) to perform or assist in the performance of Polk County business functions that will result in that person or entity creating, receiving, maintaining or transmitting ePHI on behalf of Polk County, Polk County must enter into a Business Associate Agreement with such party.

HIPAA WORKFORCE CLEARANCE POLICY

I. POLICY

The Security Officer, the Privacy Officer, or the Director of Human Relations (or their designees) will screen all members of the Workforce and other Individuals prior to granting access to ePHI.

II. PURPOSE

The purpose of this policy is to ensure that all members of the workforce have been properly cleared to gain access to ePHI and the appropriate level of access to ePHI is granted.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(3)(ii)(B)
- Information Access Management Policy

TERMINATION PROCEDURES POLICY

I. POLICY

Polk County shall terminate authorization and access rights of employees to ePHI upon termination of employment or when such access to ePHI is no longer necessary.

II. PURPOSE

The purpose of this policy is to terminate ePHI access and authorization rights for those Individuals who no longer have a need to access Polk County's ePHI.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.308(a)(3)(ii)(C)
- Authorization and/or Supervision Policy
- Information Access Management Policy

IV. SPECIFIC POLICIES UPON A WORKFORCE MEMBER'S TERMINATION

1) If a workforce member's employment is terminated or a workforce member leaves Polk County, the workforce member's supervisor or manager must ensure that all accounts to access ePHI are terminated.

2) The workforce member's supervisor or manager must ensure that access to all facilities housing ePHI has been terminated.

3) Under no circumstances will access to ePHI be extended to workforce members beyond the final date of their employment unless a Business Associate Agreement or Contract is filed in accordance to Polk County Privacy Policies.

INFORMATION ACCESS MANAGEMENT POLICY

I. POLICY

Polk County will assign each workforce member a level of access based on the Individual's need for ePHI to perform his or her job function, and will document, review, and modify as appropriate the access rights of those Individuals who have been authorized to access ePHI.

II. PURPOSE

The purpose of this policy is to ensure that access to ePHI is assigned and managed in a manner commensurate with the role of each workforce member and that access to ePHI is consistent with the HIPAA Privacy Rules.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.502(b) (Minimum Necessary Policy)
- 45 C.F.R. §164.308(a)(4)(ii)(B)
- 45 C.F.R. §164.308(a)(4)(ii)(C)
- Authorization and/or Supervision Policy
- Access Control Policy

SECURITY TRAINING POLICY

I. POLICY

All workforce members who are authorized to access ePHI are required to participate in the basic and ongoing security training.

Polk County will issue security reminders to workforce members on a periodic basis to promote awareness of security concerns and risks.

Polk County will implement and update controls to guard against, detect and report malicious code. Polk County will ensure that all system users know the dangers of, and how to respond to, viruses, worms, and other uninvited computer code that could destroy or alter system resources, including ePHI.

II. PURPOSE

The purpose of this policy is to (i) ensure that Polk County workforce is properly trained and made aware of security policies, procedures, potentials threats, and incidents; (ii) inform workforce members of security concerns on an ongoing basis; and (iii) ensure that all Polk County workforce members are appropriately made aware of the threats and vulnerabilities due to malicious code and software such as viruses and worms and are appropriately trained to identify and prevent these types of attacks.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(5)
- 45 C.F.R. §164.308(a)(5)(ii)(A)
- 45 C.F.R. §164.308(a)(5)(ii)(B)

LOG-IN MONITORING POLICY

I. POLICY

The Security Officer and/or System Administrators will monitor log-in attempts by unauthorized users and take corrective action as necessary.

II. PURPOSE

The purpose of this policy is to establish guidelines for the ongoing review and reporting of attempts at system access.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(5)(ii)(C)

PASSWORD MANAGEMENT POLICY

I. POLICY

Polk County will ensure that all user passwords that may be used to access any system or application, or to access, transmit or store ePHI are properly safeguarded.

II. PURPOSE

The purpose of this policy is to ensure that passwords created and used by Polk County workforce to access any network, system, or application used to access, transmit, receive, or store ePHI are properly safeguarded and to ensure that the workforce is made aware of all password related policies.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(a)(5)(ii)(D)
- HIPAA Security Access Control Policy

INCIDENT PROCEDURES POLICY

I. POLICY

Polk County will implement procedures for responding to and reporting suspected or known security incidents.

II. PURPOSE

The purpose of this policy is to ensure that all HIPAA security incidents and violations are appropriately identified, reported, mitigated and documented.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(6)(ii)

IV. SPECIFIC POLICIES REGARDING REPORTING INCIDENTS AND VIOLATIONS

1) A common HIPAA Incident Response and Reporting System has been setup and implemented to support the reporting, mitigation, and documentation of HIPAA security and privacy incidents and violations.

2) All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePHI must be reported.

3) Incidents that should be reported include, but are not limited to:

   a) Virus, worm, or other malicious code attacks
   b) Network or system intrusions
   c) Persistent intrusion attempts from a particular entity
   d) Unauthorized access to ePHI, ePHI based system, or ePHI based network
   e) ePHI data loss due to disaster, failure, error

BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS POLICY

I. POLICY

All agreements with business associates that create, receive, maintain, or transmit ePHI on behalf of Polk County must include security related provisions that comply with the Security Rules and HITECH.

II. PURPOSE

The purpose of this policy is to protect, through the execution and enforcement of written agreements, the privacy and confidentiality of ePHI created, received, maintained or transmitted by Polk County's business associates its behalf.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(b)
- 45 C.F.R. §164.504(e)
- Emergency Mode Operation Plan Policy
- HIPAA Privacy Policies and Procedures: Business Associate Assurances Policy

IV. POLICIES FOR ePHI EXCHANGES WITH BUSINESS ASSOCIATES

1) Polk County will identify those business associates that create, receive, maintain, or transmit ePHI and will enter into a business associate agreement with such business associate.

2) To ensure that access to critical ePHI is maintained during an emergency situation, Polk County shall implement procedures to allow caregivers necessary emergency access to ePHI necessary for individual care.

   a) This policy applies to all ePHI repositories that affect Individual care. Many repositories are not used for Individual care, and do not fall under this policy.

ADMINISTRATIVE SAFEGUARDS CONTINGENCY PLAN POLICY

I. POLICY

Polk County will develop procedures to permit access to its systems containing ePHI to Individuals who are responding to an emergency or catastrophic failure of any system, application or data, while preventing access to unauthorized personnel.

II. PURPOSE

The purpose of this policy is to establish procedures regarding facility access (i) in support of data restoration activities under the disaster recovery plan, or (ii) in the event of an emergency under the emergency mode operations plan.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(7)
- Disaster Recovery Plan Policy
- Emergency Mode Operation Plan Policy
- Authorization and/or Supervision Policy
- Data Backup Plan Policy

DATA BACKUP PLAN POLICY

I. POLICY

It is Polk County's policy to have access to retrievable, exact copies of ePHI.

II. PURPOSE

The purpose of this policy is to ensure that ePHI will not be irretrievably destroyed or lost in the event of an emergency or other occurrence.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(7)(ii)(A)
- 45 C.F.R. §164.308(a)(7)(ii)(D)
- 45 C.F.R. §164.310(d)(2)(iv)
- Integrity and Authentication Policy

DISASTER RECOVERY PLAN POLICY

I. POLICY

It is Polk County's policy to have access to backed-up and stored data and to recover any lost data in the event of a disaster or system failure.

II. PURPOSE

The purpose of this policy is to ensure that, in the event of an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing ePHI, Polk County can restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(7)(ii)(B)
- 45 C.F.R. §164.308(a)(7)(ii)(D)
- 45 C.F.R. §164.312 (a)(2)(ii)

IV. RESPONSIBILITY FOR DISASTER RECOVERY PLAN

1) The Security Officer shall be responsible for establishing and implementing the Disaster Recovery Plan.

EMERGENCY MODE OPERATION PLAN POLICY

I. POLICY

Polk County will establish and maintain procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

II. PURPOSE

The purpose of this policy is to enable continuation of critical business processes for protection of the security of ePHI after the occurrence of a disaster or other event that triggered the necessity to operate in emergency mode.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(7)(ii)(C)
- 45 C.F.R. §164.308(a)(7)(ii)(D)

IV. RESPONSIBILITY FOR EMERGENCY MODE OPERATION PROCEDURES

1) The Security Officer shall establish and implement (as needed) emergency mode operation procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

APPLICATIONS AND DATA CRITICALITY ANALYSIS

I. POLICY

Polk County will assess the relative criticality of specific software applications and data in support of other contingency plan components.

II. PURPOSE

The purpose of this policy is to provide for the security of software applications and any ePHI that is received by, stored on and/or transmitted to/from those applications.

III. REFERENCES/ CROSS REFERENCES

- 45 C.F.R. §164.308(a)(7)(ii)(E)

IV. DUTIES OF SECURITY OFFICER UNDER THIS POLICY

1) The Security Officer shall assess the relative criticality of specific software applications and data in support of other contingency plan components to ensure that critical software is accessible.

PERIODIC EVALUATION POLICY

I. POLICY

Polk County will conduct periodic evaluations to ensure that the safeguards chosen reasonably safeguard ePHI and otherwise satisfy the requirements of the Security Regulations.

II. PURPOSE

The purpose of this policy is to ensure that each Security Policy adopted by Polk County and each Security Procedure developed and implemented by a Department HIPAA Security Liaison and the Security Officer is periodically evaluated for technical and non-technical viability.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(8)

IV. GENERAL PERIODIC EVALUATION POLICY

1) Polk County Security Policies and Department Security Procedures initially should be evaluated to determine their compliance with the Security Regulations. Once compliance with the Security Regulations is established, Polk County's Security Policies and Department Security Procedures should be evaluated on a periodic basis to assure continued viability in light of technological, environmental or operational changes that could affect the security of ePHI.

FACILITY ACCESS CONTROL POLICY

I. POLICY

Polk County shall select and implement policies and procedures to safeguard all facilities, systems, and equipment used to store ePHI against unauthorized physical access, tampering, or theft.

Maintenance should be contacted for repairs. Polk County shall document and manage repairs and modifications to the physical security components of the facility.

Polk County will verify the identity of each employee performing administrative functions on behalf of Polk County or other Individual prior to granting physical access to Polk County's information systems that contain ePHI.

II. PURPOSE

The purpose of this policy is to ensure that Polk County implements physical security measures that are sufficient to secure the facilities from unauthorized physical access, tampering, and theft.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(a)(2)(ii)
- 45 C.F.R. §164.310(a)(2)(iii)
- 45 C.F.R. §164.310(a)(2)(iv)
- Authorization and/or Supervision Policy
- Risk Analysis Policy
- Risk Management Policy
- Periodic Evaluation Policy

PHYSICAL SAFEGUARDS WORKSTATION USE POLICY

I. POLICY

The workstations and other computer systems that may be used to send, receive, store or access ePHI must be used in a secure and legitimate manner.

II. PURPOSE

The purpose of this policy is to establish guidelines for the permitted uses (including the proper functions to be performed and the manner in which such functions are to be performed) of workstations of employees performing administrative functions on behalf of Polk County and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(b)
- Server, Workstation, and Mobile Systems Security Policy

SERVER, WORKSTATION, AND MOBILE SYSTEMS SECURITY POLICY

I. POLICY

Polk County will implement physical safeguards to protect workstations that contain ePHI from unauthorized access.

II. PURPOSE

The purpose of this policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store ePHI to ensure that appropriate security is maintained and that access is restricted to authorized users.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(c)
- Physical Safeguards Workstation Use Policy

IV. GENERAL SECURITY REQUIREMENTS

1) The Security Officer will ensure each server, desktop computer system and wireless computer system used to access, transmit, receive and store ePHI to ensure that appropriate security is maintained and that access is restricted to authorized users. Each workstation that is used to access, transmit, receive or store ePHI must comply with each of the aforementioned measures. If any of the aforementioned measures are not supported by the workstation operating system or system architecture, one of the following steps must be taken:

   a) The server, desktop computer system, or wireless computer system must be upgraded to support all of the following security measures,
   b) An alternative security measure must be implemented and documented, or
   c) The workstation must not be used to send, receive or store ePHI.

2) **Server Security Requirements**

   a) Each Department HIPAA Security Liaison and the Security Officer must ensure that all servers used to access, transmit, receive or store ePHI are appropriately secured in accordance with this Policy.

3) **Desktop System Security Requirements**

   a) Each Department HIPAA Security Liaison and the Security Officer must ensure that each desktop system used to access, transmit, receive or store ePHI is appropriately secured in accordance with this Policy.

4) **Mobile Systems Security Policy**

   a) Each Department HIPAA Security Liaison and the Security Officer must ensure that all mobile systems used by Workforce Members to access,

transmit, receive or store ePHI are appropriately secured in accordance with this Policy.

PHYSICAL SAFEGUARDS DEVICE AND MEDIA CONTROLS POLICY

I. POLICY

Polk County shall develop that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of such items within the facility.

II. PURPOSE

The purpose of this policy is to establish guidelines for the secure disposal of electronic media containing ePHI.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(d)(2)(i)
- 45 C.F.R. §164.310(d)(2)(ii)
- 45 C.F.R. §164.310(d)(2)(iii)

IV. APPLICATION

1) **General Application of Policy**

a) These policies and procedures pertain to the use of hard drives, storage systems, removable disks, floppy drives, CD ROMs, PCMCIA cards, memory sticks, and all other forms of removable media and storage devices.

b) The procedures developed pursuant to this Policy must be documented and submitted to the HIPAA Security Officer for approval.

ACCESS CONTROL POLICY

I. POLICY

Polk County will assign a unique name and/or number to each employee performing administrative functions on behalf of Polk County that is authorized to access ePHI and will maintain a user authentication procedure.

Polk County will safeguard ePHI through the use of automatic log off technology that terminates or suspends an electronic session after a predetermined time (15 minutes) of inactivity.

II. PURPOSE

The purpose of this policy is to ensure that authorized users are granted the level of access to information and data appropriate to their job assignments or functions and that unauthorized users are prevented from accessing any data. Assigning a unique name and/or number allows the system administrator to be able to identify and track users on the system. The purpose of this policy is also to mitigate the risk that an unauthorized user may use an authorized user's account after the authorized user has logged in.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.312(a)(2)(i)
- 45 C.F.R. §164.312(a)(2)(iii)
- 45 C.F.R. §164.312(e)
- Password Management Policy
- Physical Safeguards Workstation Use Policy
- Server, Workstation, and Mobile Systems Security Policy

TECHNICAL SAFEGUARDS AUDIT CONTROLS POLICY

I. POLICY

With the exception of emails, Polk County will employ audit controls and audit trail capabilities to record and examine activity in the system.

II. PURPOSES

The purpose of this policy is to ensure that hardware, software, and/or procedural mechanisms will be implemented by Polk County Departments, and to record and examine activity in information systems that contain or use ePHI.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.312(b)
- Information System Activity Review Policy

INTEGRITY AND AUTHENTICATION POLICY

I. POLICY

Polk County will review whether ePHI maintained on Polk County's systems has been altered or destroyed in an unauthorized manner. Polk County will educate those with access to ePHI not to alter or destroy ePHI in an unauthorized manner.

II. PURPOSES

The purpose of this policy is to ensure that ePHI maintained on Polk County's systems has not been altered or destroyed in an unauthorized manner.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.312(c)(2)
- Data Back Up Plan Policy
- Technical Safeguards Transmission Security Policy

PERSON OR ENTITY AUTHENTICATION POLICY

I. POLICY

Polk County will authenticate all persons seeking access to its ePHI and will restrict internal and external access to ePHI to authorized entities.

II. PURPOSE

The purpose of this policy is to verify the identity of the persons and entities seeking access to ePHI. Polk County shall develop to be implemented by Polk County's Security Officer and the Department HIPAA Security Liaison to verify that a person or entity seeking access to ePHI is the person or entity claimed.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.312(d)
- HIPAA Security Access Control Policy
- Password Management Policy

TECHNICAL SAFEGUARDS TRANSMISSION SECURITY POLICY

I. POLICY

Polk County will safeguard ePHI that is transmitted electronically against loss, alteration, duplication, substitution, or destruction.

II. PURPOSE

This Policy covers the technical security measures that the Security Officer will implement to guard against unauthorized access to or modification of ePHI that is being transmitted over an electronic communications network or via any form of removable media.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.312(a)(2)(iv)
- 45 C.F.R. §164.312(e)

APPENDIX A
GLOSSARY

Act means the Social Security Act.

ANSI stands for the American National Standards Institute.

Business associate: means any entity or person who, on behalf of Covered Entity (but other than in the capacity of a member of the Covered Entity's workforce), creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, Individual safety activities, billing, benefit management, practice management, and repricing, or Uses PHI to provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Covered Entity. It includes a health information organization, e-prescribing gateway or other entity or person who provides data transmission services with respect to PHI and that requires access on a routine basis to such PHI. It does not, however, include an officer, director, or employee of Covered Entity. It includes a person that offers a personal health record on behalf of the Covered Entity. It includes a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity would find it impossible to comply with both the State and federal requirements; or
(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable.

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered entity means:

(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data aggregation means, with respect to PHI created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such PHI by the business associate with the PHI received by the

business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

De-identification of PHI. A covered entity may determine that health information is not Individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not Individually identifiable:

(i) Applying such principles and methods, determines 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

(ii) Documents the methods and results of the analysis that justify such determination; or

(2) (i) The following identifiers of the Individual or of relatives, employers, or household members of the Individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, County, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) 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;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an Individual who is a subject of the information.

Designated record set refers to (1) the medical records and billing records about Individuals maintained by or for Covered Entity, or (2) any item, group, or collection of information that includes PHI and is used in whole or in part by or for Covered Entity to make decisions about Individuals.

Direct treatment relationship means a treatment relationship between an Individual and a health care provider that is not an indirect treatment relationship.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury.

The EIN is the taxpayer identifying number of an Individual or other entity (whether or not an employer) assigned under one or the following:

(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.
(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.

Employer is defined as it is in 26 U.S.C. 3401(d).

Group health plan (also see definition of health plan in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
(2) Is administered by an entity other than the employer that established and maintains the plan.

HCFA stands for Health Care Financing Administration within the Department of Health and Human Services.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an Individual.

Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an Individual or that affects the structure or function of the body; and
(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with paragraph (c)(3)(iii) of this section.

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and Individuals with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;
(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
(6) Business management and general administrative activities of the entity, including, but not limited to:
(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer.
(iii) Resolution of internal grievances;
(iv) the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual.

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of health plan in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of health plan in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health plan means an Individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(1) Health plan includes the following, singly or in combination:
(i) A group health plan, as defined in this section.
(ii) A health insurance issuer, as defined in this section.
(iii) An HMO, as defined in this section.
(iv) Part A or Part B of the Medicare program under title XVIII of the Act.
(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.
(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g) (1) of the Act, 42 U.S.C. 1395ss (g) (1)).
(vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.
(viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.
(ix) The health care program for active military personnel under title 10 of the United States Code.
(x) The veterans' health care program under 38 U.S.C. chapter 17.
(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).
(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.
(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.
(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.
(xv) The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.
(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible Individuals.
(xvii) Any other Individual or group plan, or combination of Individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) Health plan excludes:
(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg- 91(c)(1); and
(ii) A government-funded program (other than one listed in paragraph (1) (i)-(xvi) of this definition):
(A) Whose principal purpose is other than providing, or paying the cost of, health care; or
(B) Whose principal activity is:
(1) The direct provision of health care to persons; or
(2) The making of grants to fund the direct provision of health care to persons.

Hybrid entity means a single legal entity:
(1) That is a covered entity;
(2) Whose business activities include both covered and non-covered functions; and
(3) That designates health care components in accordance with paragraph (c) (3) (iii) of this section.

Implementation specification means specific requirements or instructions for implementing a standard.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an Individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and
(i) That identifies the Individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

Indirect treatment relationship means a relationship between an Individual and a health care provider in which:

(1) the health care provider delivers health care to the Individual based on the orders of another health care provider; and
(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the Individual.

Individual means the person who is the subject of PHI.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

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, who is empowered by law to:
(1) Investigate or conduct an official inquiry into a potential violation of law; or
(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited data set: A limited data set is PHI that excludes the following direct identifiers of the Individual or of relatives, employers, or household members of the Individual:

(i) Names;
(ii) Postal address information, other than town or city, State, and zip code;
(iii) Telephone numbers;
(iv) Fax numbers;
(v) Electronic mail addresses;
(vi) Social security numbers;
(vii) Medical record numbers;
(viii) Health plan beneficiary numbers;
(ix) Account numbers;
(x) Certificate/license numbers;
(xi) Vehicle identifiers and serial numbers, including license plate numbers;
(xii) Device identifiers and serial numbers;
(xiii) Web Universal Resource Locators (URLs);
(xiv) Internet Protocol (IP) address numbers;
(xv) Biometric identifiers, including finger and voice prints; and
(xvi) Full face photographic images and any comparable images.

Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the Individual, only if any payment received in exchange for making the communication is reasonably related to the cost of making the communication.
(ii) For the following purposes, except where [INSERT NAME] receives payment in exchange for making the communication:
(A) For treatment of an Individual, including case management or care coordination for the Individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the Individual;
(B) To describe a health-related product or service (or payment for such product or service) that is provided by [INSERT NAME]; or
(C) For case management or care coordination, contacting of Individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

Modify or modification refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:
(i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or
(ii) To the Individual who is the subject of the Individually identifiable health information.
(2) With respect to the rights of an Individual, who is the subject of the Individually identifiable health information, regarding access to or amendment of Individually identifiable health information, permits greater rights of access or amendment, as applicable.
(3) With respect to information to be provided to an Individual who is the subject of the Individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.
(4) With respect to the form, substance, or the need for express legal permission from an Individual, who is the subject of the Individually identifiable health information, for use or disclosure of Individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.
(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.
(6) With respect to any other matter, provides greater privacy protection for the Individual who is the subject of the Individually identifiable health information.

Organized health care arrangement means:

(1) A clinically integrated care setting in which Individuals typically receive health care from more than one health care provider;
(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
(i) Hold themselves out to the public as participating in a joint arrangement; and
(ii) Participate in joint activities that include at least one of the following:
(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if PHI created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to PHI created or received by such health insurance issuer or HMO that relates to Individuals who are or who have been participants or beneficiaries in such group health plan;
(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
(5) the group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to PHI created or received by such health insurance issuers or HMOs that relates to Individuals who are or have been participants or beneficiaries in any of such group health plans.

Payment means:

(1) The activities undertaken by:
(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the Individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Plan sponsor is defined as defined at section 3(16) (B) of ERISA, 29 U.S.C. 1002(16) (B).

PHI refers to any information, whether transmitted or maintained in electronic, written, oral, or any other form or medium, that relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present or future payment for the provision of health care to an Individual; and (i) identifies the Individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual..

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the Individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Qualified protective order means, with respect to PHI requested under paragraph (e) (1) (ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(1) Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and

(2) Requires the return to the covered entity or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

Relates to the privacy of Individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

Required by law refers to a mandate contained in law, and enforceable by a court, that compels Covered Entity to use or disclose PHI. This includes, but is not limited to, court orders, subpoenas issues by a court, grand jury, or administrative body authorized to require the production of information, and civil or investigative demands.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services or practices:
(i) Classification of components.
(ii) Specification of materials, performance, or operations; or
(iii) Delineation of procedures; or
(2) With respect to the privacy of Individually identifiable health information.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.
(2) For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

Summary health information means information, that may be Individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by Individuals for whom a plan sponsor has provided health benefits under a group health plan; and
(2) From which the information described at § 164.514(b) (2) (i) has been deleted, except that the geographic information described in § 164.514(b) (2) (i) (B) need only be aggregated to the level of a five-digit zip code.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.
(2) Health care payment and remittance advice.
(3) Coordination of benefits.

(4) Health care claim status.
(5) Enrollment and disenrollment in a health plan.
(6) Eligibility for a health plan.
(7) Health plan premium payments.
(8) Referral certification and authorization.
(9) First report of injury.
(10) Health claims attachments.
(11) Other transactions that the Secretary may prescribe by regulation.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to an Individual; or the referral of an Individual for health care from one health care provider to another.

Use means, with respect to Individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.