MENTAL HEALTH/DISABILITY SERVICES OF THE EAST CENTRAL REGION

SECURITY POLICIES AND PROCEDURES FOR COMPLIANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

"HIPAA"

TABLE OF CONTENTS

Approved June 2, 2016

Effective July 1, 2016

The following Mental Health/Disability Services of the East Central Region (Region) Security Policies apply to all County employees who are members of the Region's workforce, defined as 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." 42 CFR § 160.603. MH/DS of the East Central Region is referred to interchangeably as "Region" and "Covered Entity".

Each of the nine Counties that is a member of the Region has agreed in an amendment to the 28E agreement between the Counties that "County and its employees shall adhere to the Region's HIPAA privacy and security policies when providing services to the Region as set out in the 28E Agreement between the Region and the County."

GENERAL SECURITY COMPLIANCE

The Covered Entity is committed to conducting business in compliance with all applicable laws, regulations and the Covered Entity policies. The Covered Entity 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"), the HITECH Act of 2009, and all applicable rules and regulations, including the Final Omnibus Rule of 2013.

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

(1) Ensure the confidentiality, integrity and availability of all ePHI the Covered Entity 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 the Covered Entity 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 the Covered Entity's Workforce in relation to the protection of and authorized access to said ePHI.

Physical Safeguards--those physical measures, policies and procedures to protect the Covered Entity'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 the Covered Entity 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, the Covered Entity 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.

ASSIGNED SECURITY RESPONSIBILITY POLICY

I. POLICY

The Covered Entity 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.

The Covered Entity's HIPAA Security Officer is Deborah L. Seymour-Guard.

II. PURPOSE

The purpose of this policy is to establish the duties and responsibilities of the Security Officer.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.308(a)(2)

IV. PROCEDURES

1) The Security Officer shall oversee the development, implementation and operation of Covered Entity's HIPAA Security Program. The Security Officer shall have the following responsibilities:

   a) Report to the Chief Executive Officer (CEO) of Covered Entity, who will in turn report to the Governing Board with respect to all actions and recommendations of the Security Officer.

   b) Develop and revise as needed the Covered Entity's HIPAA Security Policies and Procedures to address security threats and vulnerabilities to the confidentiality, integrity and availability of ePHI.

   c) In conjunction with the Privacy Officer, participate in periodic risk assessments of the security and privacy of PHI, including Covered Entity's ePHI.

   d) Answer questions from members of Covered Entity's workforce concerning the ePHI security safeguards, policies and procedures.

   e) Prepare cost benefit analyses of appropriate ePHI safeguards and make recommendations regarding the adoption of safeguards.

   f) Prepare the annual budget for ePHI security.

g) Meet with appropriate Individuals, including the Privacy Officer and the CEO, to discuss ePHI security issues, policies and planning.

h) Ensure that all ePHI security policy and procedure manuals and materials are kept up to date and current with government rules, regulations and practices.

i) Monitor Covered Entity's compliance with applicable ePHI security laws and regulations; monitor compliance with Covered Entity's HIPAA Security Policies and Procedures among members of Covered Entity's workforce and other third parties.

j) 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.

k) Develop an appropriate ePHI security training program for members of the Covered Entity's workforce in conjunction with the Privacy Officer.

l) Prepare and periodically assess Covered Entity's security incident response procedures, disaster recovery plan and business continuity plan for information systems containing ePHI.

m) Perform security audits of ongoing system activities utilizing ePHI.

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

o) In conjunction with the Privacy Officer, investigate violations of Covered Entity's HIPAA policies.

p) Consistent with Covered Entity's Sanctions policy, in the event it is determined that a member of Covered Entity's workforce has violated Covered Entity's HIPAA policies, make recommendations in conjunction with the Privacy Officer to the County Employer of the workforce member concerning appropriate discipline of the workforce member.

q) In conjunction with the Privacy Officer, facilitate a process for Individuals to file a complaint regarding the Covered Entity's Security Policies or the handling of ePHI by the Covered Entity, including ensuring that the complaint and its disposition are appropriately documented.

r) Coordinate with the Privacy Officer regarding the mitigation of the effects of any unauthorized or otherwise inappropriate release of health information.

s) On a periodic basis, report the status of security compliance to the Governing Board in conjunction with the CEO, as appropriate.

t) Serve as a liaison with other entities, including the Iowa State Association of Counties with respect to HIPAA compliance.

RISK ANALYSIS POLICY

I. POLICY

The Covered Entity acknowledges the potential vulnerabilities associated with storing ePHI, transmitting ePHI locally, transmitting ePHI outside of the Covered Entity, and transmitting ePHI to the Covered Entity's workforce members. The Covered Entity 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 Covered Entity maintains.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.308(a)(1)(ii)(A)

IV. PROCEDURES

1) The Security Officer shall at least once a year:

   a) Identify and document all ePHI repositories (i.e., any location in which ePHI is kept, 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) All repositories of ePHI will be identified and logged into a common catalogue. An ePHI repository may be in the form of a database, spreadsheet, folder, storage device, document or other form of electronic information that is accessed by one or more users. Each repository will be logged with the appropriate level of file, system, and owner information including, but not limited to:

   a) Repository Name
   b) Custodian Name
   c) Custodian Contact Information

d) Number of Users that access the repository
e) Number of Records
f) System Name
g) System Location
h) System Manager Contact Information
i) Risk Level

3) The Security Officer and each Member County of the Covered Entity shall update the ePHI inventory as needed to ensure that the ePHI catalogue is up to date and accurate. Each identified ePHI repository will be analyzed for any potential vulnerability to the integrity, confidentiality, and availability of its ePHI. The following two-dimensional model will be used to assign a risk level to each ePHI repository:

a) High Risk – Repositories with a large number of records accessed by a large numbers of users
b) Medium Risk – Repositories with either a large number of records and a small number of users or a small number of records and a large number of users
c) Low Risk – Repositories with a small number of records accessed by a small number of users

4) Each Member County 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.

5) 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 Covered Entity Security Officer.

RISK MANAGEMENT POLICY

I. POLICY

The Covered Entity 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 Covered Entity 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)

IV. PROCEDURES

1) The level, complexity and cost of such security measures and safeguards shall be commensurate with the risk classification of each such ePHI repository. The Covered Entity shall meet the following minimum guidelines in implementing security measure and safeguards:

    a) Low risk ePHI repositories may be appropriately safeguarded by normal best-practice security measures in place such as user accounts, passwords and perimeter firewalls.
    b) Medium and high risk ePHI repositories must be secured in accordance with HIPAA Security Policies and Procedures.

2) Covered Entity will evaluate the following factors when selecting and implementing administrative, physical and technical security safeguards:

    a) The size, complexity, and capabilities of Covered Entity;
    b) Covered Entity's technical infrastructure, hardware, and software security capabilities;
    c) The costs of the security measures;
    d) The probability and criticality of potential risks to ePHI;
    e) The feasibility of implementation and use (e.g., compatibility, user acceptance); and
    f) The effectiveness (e.g., degree of protection and level of risk mitigation) of the mechanism, process or safeguard.

3) Covered Entity will assign appropriate Workforce members or external staff who possess the requisite expertise and skill sets to implement the selected security safeguards.

4) To the extent possible, Covered Entity will schedule the implementation of appropriate security safeguards without undue disruption to business operations.

5) To the extent the Security Officer reassesses the potential risks and vulnerabilities of an ePHI repository as part of a periodic review, the Security Officer shall update the security measures and safeguards for such ePHI repository to reflect any changes in the risks and vulnerabilities assessment.

SANCTIONS POLICY

I. POLICY

Covered Entity has established and will apply appropriate sanctions against members of its workforce, as well as other agents and contractors, who fail to comply with its HIPAA Privacy and Security policies and procedures.

II. PURPOSE

This Policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to sanctions for violating Covered Entity's HIPAA Privacy and Security policies and procedures.

III. REFERENCE/CROSS-REFERENCE

- 45 C.F.R. §164.530(e)
- 45 C.F.R. §164.308(a)(1)(ii)(C)

IV. PROCEDURE

A. General Rule Regarding Sanctions. All workforce members shall comply with the written policies and procedures included in the Privacy and Security Manuals as amended from time to time concerning Covered Entity's PHI. Pursuant to the HIPAA Confidentiality Addendum to 28E Agreement between Covered Entity and its member Counties, a violation of the HIPAA Privacy or Security Rules or Covered Entity's Privacy or Security policies shall result in an appropriate sanction by the appropriate County against its employee consistent with County's human resources policies and procedures [and applicable collective bargaining agreements], consistent with Covered Entity's investigation and recommendations. The type and severity of the sanction applied by County shall depend on whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors. Sanctions could range from verbal reprimand to termination.

Members of Covered Entity's workforce should be aware that violations may result in notification to law enforcement officials, Individuals whose PHI is inappropriately access, acquired, used or disclosed, as well as to regulatory, accreditation, and/or licensure organizations.

B. General Process for Responding to Possible Violations.

1) Members of Covered Entity's workforce are required to report any possible Privacy or Security violation of Covered Entity's PHI to Covered Entity's Privacy Officer or Security Officer.

2) Each County shall have an obligation to report to Covered Entity any possible Privacy or Security Violation of Covered Entity's PHI by one of its employees of which it knows or has reason to know as soon as practicable.

3) Whenever possible Privacy Violations arise, the Privacy Officer shall conduct an investigation and determine whether a violation has occurred by a member of its workforce; if a possible Security Violation arises, the Security Officer shall conduct the investigation and make a determination whether a violation has occurred. Where appropriate, the Privacy Officer and the Security Officer should conduct a joint investigation.

4) Covered Entity's Privacy or Security Officer shall report to the Employer of the member of Covered Entity's workforce the results of any investigation concerning the workforce member. In the event that it is determined there has been a Privacy Violation or a Security Violation, the Privacy or Security Officer shall make a recommendation to the Employer concerning appropriate discipline. The Employer shall impose an appropriate sanction against Covered Entity's workforce member consistent with Employer's human resources policies and procedures and applicable collective bargaining agreements.

5) In addition to any discipline imposed by County, for any Security or Privacy violation, Covered Entity shall have the discretion to request that the member of its workforce be replaced by another County employee if feasible.

6) A record of the incident, investigation, and any discipline imposed by the County shall be maintained by the Privacy Officer or Security Officer as appropriate for a period of six years.

C. Mitigation. The Covered Entity shall mitigate, to the extent practicable, any harmful effect known to the Covered Entity of a use or disclosure of PHI in violation of its policies and procedures by the Covered Entity workforce members or by its business associates.

D. Examples of HIPAA Violations Which May Result in Sanctions

- Accessing information that you do not need to know to do your job;
- Sharing your computer access codes (user name & password/using another person's computer access codes [user name & password]);
- Leaving your computer unattended while you are logged into a PHI program;
- Sharing PHI with another employee without authorization;
- Copying PHI without authorization;
- Changing PHI without authorization;
- Discussing confidential information in a public area or in an area where the public could overhear the conversation;
- Discussing confidential information with an unauthorized person;
- Failing to cooperate with the Covered Entity's Privacy and/or Security Officer;

- Any unauthorized use or disclosure of PHI;
- Failing to comply with mitigation decisions;
- Obtaining PHI under “false pretenses”; or
- Using and/or disclosing PHI for commercial advantage, personal gain or malicious harm.

INFORMATION SYSTEM ACTIVITY REVIEW POLICY

I. POLICY

The Covered Entity 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 tracking reports.

III. REFERENCES/CROSS REFERENCES

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

IV. PROCEDURES

1) To ensure that system activity for all systems classified as medium and high risk is appropriately monitored and reviewed, the Security Officer shall follow the minimum procedures outlined below:

   a) An internal audit procedure has been established and implemented by each County and the Security Officer to regularly review records of system activity. The internal audit procedure utilizes audit logs, activity reports, and other mechanisms to document and manage system activity.

   b) Audit logs, activity reports, and other mechanisms to document and manage system activity are reviewed at intervals commensurate with the associated risk of the information system or the ePHI repositories contained on said information system.

   c) At a minimum, Covered Entity will review login IDs, dates, times, and session times so as to identify:

      i. unauthorized access and/or attempts to access to ePHI;
      ii. unauthorized modification of and attempts to modify ePHI;
      iii. attempts to exceed access authority;
      iv. attempts to gain system access during unusual hours;
      v. unusual levels of activity that are inconsistent with a workforce member's job functions; and
      vi. sustained activity levels for extended periods of time, inconsistent with a workforce member's scheduled work hours.

   d) Security incidents such as activity exceptions and unauthorized access attempts if they occur will be detected, logged and reported immediately

to the appropriate Department HIPAA Security Liaison and the Security Officer in accordance with the HIPAA Security Incident Response and Reporting Policy.

e) The Covered Entity will undertake corrective action and will implement additional security safeguards as appropriate and consistent with the Risk Management Policy and Security Incident Procedures Policy.

AUTHORIZATION AND/OR SUPERVISION POLICY

I. POLICY

Covered Entity will authorize members of Covered Entity's workforce 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)
- Workforce Clearance Policy
- Access Control and Validation Procedures Policy

IV. PROCEDURES

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

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

3) Security Officer will maintain a list of those employees who require access to and are authorized to access ePHI.

HIPAA WORKFORCE CLEARANCE POLICY

I. POLICY

The County Employer shall screen its employees who are members of Covered Entity's workforce and shall provide results of such screening to Covered Entity.

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

IV. PROCEDURES

1) A background check must be performed by the County Employer on all workforce members requiring access to ePHI repositories and the results provided to the Security Officer. The background check must be completed and deemed satisfactory by the Security Officer before access to high risk ePHI is granted.

2) All employees must complete the security training program, within two months of hire, in order to obtain authorization and access rights to ePHI.

3) Each County must comply with the policies and procedures for authorizing, managing, and terminating access to ePHI for Covered Entity's workforce members detailed in HIPAA Security Information Access Management Policy.

4) All the Covered Entity workforce members are subject to the attached Covered Entity Code of Conduct as it relates to the appropriate use of PHI and ePHI. The County Employer shall have the responsibility for providing the Code of Conduct to its employees who are members of Covered Entity's workforce.

ATTACHMENT TO WORKFORCE CLEARANCE POLICY

Covered Entity Code of Conduct

This code applies to:

1) Members of the Covered Entity's workforce;

2) Consultants, vendors, and contractors when they are doing business with the Covered Entity; and

3) Individuals who perform services for the Covered Entity as volunteers.

The Code of Conduct refers to all these persons collectively as "members of the Covered Entity community" or "community members."

Integrity and Ethical Conduct. The Covered Entity is committed to the highest ethical and professional standards of conduct as an integral part of its mission. To achieve this goal, the Covered Entity relies on each community member's ethical behavior, honesty, integrity, and good judgment. Each community member should demonstrate respect for the rights of others. Each community member is accountable for his or her actions. This Code of Conduct describes standards to guide us in our daily Covered Entity activities.

Compliance with Laws and Covered Entity Policies. The Covered Entity and each community member must transact Covered Entity business in compliance with all laws, regulations, and Covered Entity policies related to their positions and areas of responsibility.

Procedures for Reporting Violations or Concerns. The Covered Entity's compliance effort focuses mainly on teaching members of the Covered Entity community the appropriate compliance standards for the areas in which they work. Nevertheless, violations may occur. In addition, members of the Covered Entity community may have concerns about matters that they are not sure represent violations. Each community member is expected to report violations or concerns about violations of this Code of Conduct that come to his/her attention to Covered Entity's Privacy Officer or Security Officer. The Privacy Officer and/or Security Officer shall investigate any possible violation of this Code of Conduct, the Privacy and Security Rules, or Covered Entity's Privacy or Security Policies. If a violation is confirmed, the Covered Entity shall make a recommendation to the County or other entity that employs the workforce member with respect to discipline, consistent with Covered Entity's sanctions policy. Individuals who violate the Code may also be subject to civil and criminal charges in some circumstances.

How to Report a Violation or Discuss a Concern. You may report violations or concerns to the Privacy Officer at 319-325-1919 x104 or the Security Officer at 319-668-5810. Reports may be made anonymously to this number, if the caller so desires.

TERMINATION PROCEDURES POLICY

I. POLICY

Covered Entity shall terminate authorization and access rights of workforce members to ePHI upon termination of the association between the Covered Entity and the workforce member 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 Covered Entity'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. PROCEDURES

1) If a workforce member's association with the Covered Entity is terminated for any reason, including but not limited to termination by the individual's County Employer, the workforce member's supervisor or manager at his or her County of employment shall report the change to the Security Officer and the Security Officer shall ensure that all accounts to access ePHI are terminated.

2) Security Officer shall ensure that all access to Covered Entity's e-mail, Sharepoint and CSN services are terminated.

3) Under no circumstances will access to ePHI be extended to workforce members beyond the final date of their employment with his or her County of employment, unless a Business Associates Arrangement or Contract is filed in accordance to the Covered Entity Privacy Policies.

ATTACHMENT TO TERMINATION PROCEDURES POLICY

TERMINATION CHECK LIST

Employee Name: _____ Department: _____

Actual Last Day Worked: _____ Division: _____

Upon notification of an employee's termination, the Security Officer should be contacted immediately by the employee's supervisor. The following items (if applicable) must be collected by the employee's immediate supervisor and sent to the appropriate Individual for processing.

COMPUTER SECTION

[ ] User Name Account Disabled [ ] Remote Access Disabled [ ] Sharepoint Access
[ ] Email Disabled [ ] Other_____
Notes: _____

Former Employee's Forwarding Address:

Street Address: _____
City/State/Zip: _____
Phone Number: (___) _____

_____Date:_____
Signature of Immediate Supervisor indicating receipt of above information:

_____Date:_____
Security Officer's Signature

I acknowledge that I am no longer to access any information or accounts nor will I utilize any information that I already know in violation of HIPAA.

_____Date:_____
Signature of former workforce member

INFORMATION ACCESS MANAGEMENT POLICY

I. POLICY

The Covered Entity 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 Establishment and Modification Policy

IV. PROCEDURES

1) The Security Officer must implement procedures to establish, document, review and modify each workforce member's right to access ePHI. These procedures include the following responsibilities:

   a) It is the responsibility of Covered Entity to authorize access to systems and networks containing ePHI for each workforce member. Workforce members are not permitted to authorize their own access to ePHI or be granted authorization from anyone else.

   b) It is the responsibility of the Security Officer to ensure that Covered Entity's ePHI meets the minimum requirements for their roles.

   c) It is the responsibility of the Security Officer to review the access granted to ePHI for each member of the workforce and adjust their access rights as their roles changed.

   d) It is the responsibility of the workforce member's County employer to report a change of status of a workforce member to Security Officer as soon as possible.

2) The Security Officer may conduct further background checks into workforce member's background before allowing the workforce member access to ePHI, including but not limited to credit history checks, criminal record checks and employment history verification

3) The Security Officer may modify a workforce member's access to ePHI in his or her discretion.

4) The Security Officer will maintain an inventory of users authorized to access ePHI.

5) The Security Officer will document any changes to a user or workforce member's access rights on the inventory of users.

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 provided by his or her County Employer and/or Covered Entity.

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

Covered Entity will implement and update controls to guard against, detect and report malicious code. County Entity 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 with respect to their electronic assets. Covered Entity shall educate members of its workforce with respect to controls for SharePoint and Microsoft Office 365.

II. PURPOSE

The purpose of this policy is to (i) ensure that the Covered Entity 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 Covered Entity 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)

IV. PROCEDURES

1) HIPAA Security Training.

a) Members of Covered Entity's workforce that access, receive, transmit, or otherwise use ePHI or set up, manage, or maintain systems and workstations that access, receive, transmit, or store ePHI are subject to HIPAA Security Training.

b) To ensure that all Covered Entity workforce members are appropriately made aware of all HIPAA Security Policies and Procedures and their responsibilities in relation to understanding and complying with the HIPAA Security Policies and Procedures, the following training procedures must be established and implemented:

i. The Security Officer in collaboration with the Privacy Officer is responsible for ensuring that its workforce has the appropriate level of HIPAA Privacy training.

ii. The Security Officer is responsible for ensuring that its workforce has the appropriate level of HIPAA Security Training with respect to systems maintained by Covered Entity, including Microsoft Office 365 and SharePoint. The minimum level of HIPAA Security training must consist of, but is not limited to, the following requirements:

1. HIPAA Security Policies
2. HIPAA Sanction Policy
3. Confidentiality, Integrity, and Availability (CIA)
4. Individual security responsibilities
5. Common security threats and vulnerabilities

iii. With respect to systems that the Covered Entity controls, including Microsoft Office 365 and SharePoint, the Security Officer must also ensure that the workforce is aware of and trained to comply with the following HIPAA Security policies and procedures:

1. Login Monitoring procedures (See HIPAA Security Training and Awareness Policy)
2. Audit Control and Review Plan (See HIPAA Security Audit Control Policy)
3. Data Backup Plan (See HIPAA Security Contingency Planning Policy)
4. Disaster Recovery Plan (See HIPAA Security Contingency Planning Policy)

iv. The Security Officer must maintain formal documentation of the current level of HIPAA training for each of its workforce members.

v. The Security Officer shall seek and maintain copies of County Employers' security and privacy policies. The Security Officer shall seek and maintain copies of risk analyses performed by County.

2) Security Reminders.

a) The Security Officer is responsible for ensuring that its workforce is made aware of all changes or updates to HIPAA security policies and procedures.

b) The Security Officer must establish and implement a procedure to disseminate security reminders to its workforce to make them aware of any of the following events:

i. A new HIPAA Security Policy or Procedure has been approved.
ii. A current HIPAA Security Policy or Procedure has been updated.
iii. A new threat, breach or vulnerability has been discovered or reported that may affect ePHI. (See HIPAA Security Incident Response and Reporting Policy)

3) Protection from Malicious Software

For systems, applications, and networks that Covered Entity controls:

a) The Security Officer is responsible for ensuring that Covered Entity's workforce is appropriately trained to identify and protect against malicious code and software.
b) The Security Officer shall disseminate security reminders to Covered Entity's workforce to make them aware of any new virus, worm, or other type of malicious code that may be a threat to ePHI maintained on systems controlled by Covered Entity.
c) The appropriate County personnel shall notify the HIPAA Security Officer in the event that a virus, worm, or other malicious code has compromised or potentially compromised ePHI.
d) The Security Officer must notify the County IT Department in the event that a virus, worm, or other malicious code has been identified and is a potential threat to other systems or networks. (See HIPAA Security Incident Response and Reporting Policy)
e) In the event that a virus, worm, or other malicious code has infected or been identified on a server or workstation, that system must be disconnected from the network until the system has been appropriately cleaned.

LOG-IN MONITORING POLICY

I. POLICY

The Security Officer 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)

IV. PROCEDURES

1) The Security Officer will monitor log-ins and other attempts at system access.

2) All system users are required to report to the Security Officer or appropriate designee, any suspicious log-in activity, log-in attempts, or other discrepancies.

PASSWORD MANAGEMENT POLICY

I. POLICY

For systems, applications or networks that Covered Entity controls, i.e., SharePoint and Microsoft Office 365, the Covered Entity 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 the Covered Entity workforce to access networks, systems, or applications it controls that are 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)

IV. PROCEDURES

1) **Password Management**

a) For systems, applications and networks that Covered Entity controls, all workforce members must be supplied with a Unique User Identification to access the aforementioned ePHI.

b) For systems, applications, and networks that Covered Entity controls, all workforce members must supply a password in conjunction with their Unique User Identification to gain access to any application or database system used to create, transmit, receive, or store ePHI.

c) All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store ePHI must be of sufficient complexity to ensure that it is not easily guessable.

d) For systems, applications, and networks that Covered Entity controls, managers of networks, systems, or applications used to access, transmit, receive, or store ePHI must ensure that passwords set by workforce members meet the minimum level of complexity as defined in HIPAA Security Password Structure Policy.

f) Password aging times shall be implemented in a manner commensurate with the criticality and sensitivity of the ePHI contained within each network, system, application or database but shall not be longer than 90 days.

g) Workforce members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:

i. Passwords are only to be used for legitimate access to networks, systems, or applications.
ii. Passwords must not be disclosed to other workforce members or individuals.
iii. Workforce members must not allow other workforce members or individuals to use their password.
iv. Passwords must not be written down, posted, or exposed in an unsecured manner such as on a notepad or posted on the workstation or under the keyboard.

h) If a workforce member knows that the confidentiality of his or her password for any Entity controlled software has been compromised, he or she must contact the Security Officer immediately. The Security Officer will enable the workforce member to set a new and different password.

INCIDENT PROCEDURES POLICY

I. POLICY

The Covered Entity 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. PROCEDURES

1) A HIPAA Incident Response and Reporting System has been set up 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 using the following procedure:

   Users must notify the Security Officer or Privacy Officer for issues involving viruses, local attacks, Denial of Service (DOS) attacks, etc. Users must also notify their County IT Department or IT Contractor of any such issues.

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, or error

4) The HIPAA Security Officer shall notify the appropriate County personnel if a security incident involves an outside entity or traverses the network.

5) The County Coordinator of Disability Services must notify the HIPAA Security Officer if they are notified of or detect an incident they feel may impact Covered Entity's ePHI systems or data.

6) All HIPAA related incidents, security and privacy, must be logged and documented by the HIPAA Security and/or Privacy Officers. The HIPAA Security Officer must notify members of the workforce of Policy Updates and Changes, Virus or other malicious software updates, Covered Entity-wide threats to ePHI, etc. As appropriate, the Security and/or Privacy Officers shall provide Policy Updates and Changes, Virus or other malicious software updates, Covered Entity-wide threats to ePHI, etc. to County IT personnel.

7) Disaster Recovery reporting procedures must include the following:

   a) All instances of failures, outages, or data loss that involve critical ePHI must be logged internally within the Covered Entity (See HIPAA Security Contingency Planning Policy).
   b) All instances of failures, outages, or data loss that involve critical ePHI must be reported to the HIPAA Security Officer.
   c) All correspondence with outside authorities such as local police, FBI, media, etc. must go through the Covered Entity Attorney, the applicable County Coordinator of Disability Services and the Security Officer.

BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS POLICY

I. POLICY

All agreements with business associates that create, receive, maintain, or transmit ePHI on behalf of Covered Entity 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 Covered Entity's business associates on its behalf.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164. 164.308(b)
- 45 C.F.R. §164.504(e)
- Emergency Mode Operation Plan Policy
- HIPAA Privacy Policies and Procedures: Business Associate Policy

IV. PROCEDURES

Covered Entity will identify those business associates that create, receive, maintain, or transmit Covered Entity's ePHI and will enter into a business associate agreement with such business associate that includes:

a) language that requires the business associate to comply with the Security Rule's administrative, technical and physical safeguards and policies and procedure requirements in the same manner as the requirements apply to the plan;

b) provisions that ensure that any agent, including a subcontractor, to whom the business associate provides the ePHI agrees to implement reasonable and appropriate safeguards;

c) provisions that require the business associate to report to Covered Entity certain security incidents of which the business associate becomes aware;

d) provisions that authorize termination of the contract by Covered Entity if Covered Entity determines that the business associate has violated a material term of the contract.

ADMINISTRATIVE SAFEGUARDS CONTINGENCY PLAN POLICY

I. POLICY

Covered Entity 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. §164.310(a)(2)(i)
- Disaster Recovery Plan Policy
- Emergency Mode Operation Plan Policy
- Authorization and/or Supervision Policy

IV. PROCEDURES

1) Covered Entity will identify those Individuals and systems required for the business to function.

2) The Security Officer shall develop procedures for alternate access to critical systems by appropriate personnel.

3) The Security Officer shall develop procedures for restoring data and functionality after the event that causes the contingency operations.

4) The assessment of data and application criticality shall be conducted periodically to ensure that appropriate procedures are in place for data and applications at each level of risk.

DATA BACKUP PLAN POLICY

I. POLICY

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.

II. PURPOSE

It is Covered Entity's policy to have access to retrievable, exact copies of ePHI.

III. REFERENCES/CROSS REFERENCES

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

IV. PROCEDURES

1) Data Backup Plan

a) For all Covered Entity ePHI, the Security Officer has established and implemented a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all ePHI determined to be medium and high risk.

b) The Data Backup Plan applies to all medium and high risk files, records, images, voice or video files that may contain ePHI.

c) The Data Backup Plan requires that all media used for backing up ePHI be stored in a physically secure environment, including a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.

d) The Data Backup Plan factors in the cost of the backup and the likelihood of inability to function in the event that the data was lost.

e) The Security Officer will determine which information must be retrievable for Covered Entity to continue to function as usual in the event of damage or destruction of the data, hardware, or software.

f) Data backup procedures outlined in the Data Backup Plan must be tested on a periodic basis to ensure that exact copies of ePHI can be retrieved

2) Off-Site Storage Facility or Backup Service. When an off-site storage facility or backup service is used, a written contract or Business Associate Agreement is used to ensure that the Business Associate will safeguard the ePHI in an appropriate manner.

DISASTER RECOVERY PLAN POLICY

I. POLICY

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, Covered Entity can restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner.

II. PURPOSE

It is Covered Entity'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.

III. REFERENCES/CROSS REFERENCES

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

IV. PROCEDURES

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

2) Disaster Recovery Plan Requirements

a) The Disaster Recovery Plan includes procedures to restore ePHI from data backups in the case of a disaster causing data loss.

b) The Disaster Recovery Plan includes procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

c) The Disaster Recovery Plan, at a minimum, contains the following requirements:

i. Covered Entity will conduct a daily backup
ii. The daily backup will only backup changes from the previous day
iii. Each Friday, a full system backup shall be conducted
iv. The daily backup tape will be kept onsite, but in a different, physically secure room from other servers
v. The weekly backup shall be kept at any offsite, secure location designed specifically for the purpose of storing backup data.

d) The Disaster Recovery Plan is documented and easily available to the necessary personnel at all times, who are trained to implement the Disaster Recovery Plan.

e) The disaster recovery procedures outlined in the Disaster Recovery Plan are tested on a periodic basis to ensure that ePHI and the systems needed to make ePHI available can be restored or recovered.

EMERGENCY MODE OPERATION PLAN POLICY

I. POLICY

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.

II. PURPOSE

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

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(7)(ii)(C)

IV. 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.

2) Emergency mode operation procedures outlined in the Emergency Mode Operation Plan shall be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

APPLICATIONS AND DATA CRITICALITY ANALYSIS

I. POLICY

Covered Entity 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. PROCEDURES

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. Such a plan shall consider:

   a) The physical and technical security of data and ePHI
   b) Access to data and critical networks, software and hardware in the event of emergency;
   c) Critical business functions.

PERIODIC EVALUATION POLICY

I. POLICY

The Covered Entity 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 the Covered Entity is periodically evaluated for technical and non-technical viability.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(8)

IV. PROCEDURES

1) Periodic Evaluation Generally. The Covered Entity Security Policies should be evaluated to determine their compliance with the Security Regulations. Once compliance with the Security Regulations is established, the Covered Entity Security Policies 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. Following the initial risk analysis performed by Covered Entity in 2015, County shall be responsible for periodic evaluation of the security of County ePHI, and shall provide a copy of the risk assessments it performs on a periodic basis to Covered Entity.

2) Periodic Evaluation by the Covered Entity HIPAA Security Officer

a) The HIPAA Security Officer will review on an on-going basis the viability of the Covered Entity Security Policies and general approaches taken by Coordinators of Disability Services in their Security Procedures.

b) The HIPAA Security Officer will develop and recommend to the Regional Governing Board any necessary Security Policy or Security Procedure changes.

3) Evaluation upon Occurrence of Certain Events

a) In the event that one or more of the following events occur, the Privacy and Security Officers shall reevaluate the Covered Entity's policies.

i. Changes in the HIPAA Security Regulations or Privacy Regulations

ii. New federal, state, or local laws or regulations affecting the privacy or security of PHI

iii. Changes in technology, environmental processes or business processes that may affect HIPAA Security Policies or Security Procedures

iv. A serious security violation, breach, or other security incident occurs

PHYSICAL SAFEGUARDS WORKSTATION USE POLICY

I. POLICY

It is the Region's expectation that each member County shall ensure that 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 Covered Entity members performing administrative functions on behalf of Covered Entity 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)
- Workstation Security Policy

IV. PROCEDURES

1) Compliance with the Covered Entity Computer Use Policy

To ensure that workstations and other computer systems that may be used to send, receive, store or access ePHI are only used in a secure and legitimate manner, Workforce members who, and workstations and other computer systems that are used to, send, receive, store and access ePHI must comply with the Covered Entity Computer Use Employee Handout, a copy of which is attached hereto.

2) The Covered Entity Monitoring of Workstation Use

Workforce members that use the Covered Entity information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, the Covered Entity may log, review, or monitor any data (ePHI and non-ePHI) stored or transmitted on its information system assets.

3) Removal of Workforce Members Privileges

The Covered Entity may remove or deactivate any Workforce member's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

THE FOLLOWING SHALL BE PROVIDED TO COUNTY EMPLOYERS FOR CIRCULATION TO EMPLOYEES WHO ARE MEMBERS OF COVERED ENTITY'S WORKFORCE

ATTACHMENT TO PHYSICAL SAFEGUARDS WORKSTATION USE POLICY

The Covered Entity Computer Use Handout

Introduction

This document offers principles to help guide members of the Covered Entity community, and specific policy statements that serve as a reference points. It will be modified as new questions and situations arise.

While the proliferation of computers and information technologies does not alter basic codes of behavior, it does place some issues in new contexts. Using these technologies enables people to do varied things-both good and bad-more easily. They are an enormously rich resource for innovation in the furtherance of the Covered Entity's mission. But they increase the risks of actions, deliberate or not, that are harmful in various ways, including: (a) interference with the rights of others; (b) violation of the law; (c) interference with the mission of the Covered Entity; or (d) endangering the integrity of the Covered Entity's information computer network. The guidelines that follow seek to forge the link between established codes of conduct and use of new technologies. Computer networking has greatly expanded our ability to access and exchange information, requiring more vigilant efforts and perhaps more secure safeguards to protect Individuals' rights of privacy. Property as well as privacy rights may be infringed whenever files or data belonging to others, however gained, are used without authorization; moreover, while freedom of inquiry and expression are fundamental principles of life, assaults upon the personal integrity of Individual members of the community and dissemination of offensive materials may undermine the foundations of that community. Other actions taken by Individuals may, under some circumstances, jeopardize the integrity of the computer network and the ability of others to communicate using this system. Accordingly, the guidelines that follow seek to both preserve the freedom to inquire and share information and sustain the security and integrity of Individuals within the community and the computer system itself.

While some of the guidelines therefore call for respectful and responsible use of the computer networks to protect the rights of Individuals, others warn against actions that may violate the law: users within the community must understand the perils of illegal use, exchange, or display of copyrighted, deceptive, defamatory, or obscene materials on a web page or through other electronic communication channels.

The community at large has rights and expectations that must be considered. When Individuals misrepresent either themselves or the Covered Entity, or when they act by computer in a manner unacceptable within the Covered Entity or in the larger community, the integrity and mission of the Covered Entity itself is endangered.

Finally, the guidelines seek to protect the integrity of the Covered Entity information systems themselves: the computing or networking resources need to be accessible and secure for appropriate uses consistent with the mission of the Covered Entity; the usurpation of these resources for personal gain or without authorization is unacceptable. Moreover, even the Individual right to privacy may, when personal files may need to be accessed for troubleshooting purposes, be overridden by authorized personnel to protect the integrity of the Covered Entity's computer systems.

Principles and Guidelines

As a threshold matter, when you are conducting Covered Entity business, you must encrypt any message containing PHI.

A. Respect the rights and sensibilities of others

1. Electronic mail should adhere to the same standards of conduct as any other form of mail. Respect others you contact electronically by avoiding distasteful, inflammatory, harassing or otherwise unacceptable comments.
2. Others have a right to know who is contacting them.
3. Respect the privacy of others and their accounts. Do not access or intercept files or data of others without permission. Do not use the password of others or access files under a false identity.
4. Distribution of excessive amounts of unsolicited mail is not allowed.
5. While the Covered Entity encourages respect for the rights and sensibilities of others, it cannot protect Individuals against the existence or receipt of materials that may be offensive to them. Those who make use of electronic communications may come across or be recipients of material they find offensive or simply annoying.

B. Be aware of the legal implications of your computer use.

1. The Internet enables users to disseminate material worldwide. Thus the impact of dissemination on the internet is often far broader than that of a statement made on paper or in routine conversation. Keep in mind that a larger audience means a greater likelihood that someone may object with or without legal basis.
2. Much of what appears on the internet is protected by copyright law regardless of whether the copyright is expressly noted. Users should generally assume that material is copyrighted unless they know otherwise and not copy or disseminate copyrighted material without permission. Copyright protection also applies to much software, which is often licensed to the Covered Entity with specific limitations on its use. Both Individual users and the Covered Entity may, in some circumstances, be held legally responsible for violations of copyright.
3. Many other state and federal laws, including those prohibiting deceptive advertising, use of others' trademarks, defamation, violations of privacy, and obscenity, apply to network-based communications.

C. Respect the mission of the Covered Entity in the larger community

1. The Covered Entity makes internet resources available to staff to further the Covered Entity's service and related missions. While incidental personal use is permissible in most settings, these resources are generally available only for Covered Entity-related activities.
2. The Covered Entity may monitor the content of web pages, electronic mail or other on-line communications. Under certain circumstances, the Covered Entity may be held liable if it fails to take reasonable remedial steps after it learns of illegal uses of its computer facilities. Use computer resources lawfully.

3. Remember that you are responsible for all activity involving your account. Keep your account secure and private. Your password should be difficult to crack or otherwise guess either by Individuals or by sophisticated computer programs.

4. Respect the Covered Entity obligations of confidentiality as well as your own. Only those with authorization may access, communicate or use confidential information.

5. Material posted on web pages is generally accessible and thus deserves even greater thought and care than your private electronic mail. Remember that, absent restrictions, your web page is available to anyone, anywhere, and act accordingly.

6. The Covered Entity has a right to expect that computer users will properly identify themselves. Computer accounts are assigned and identified to Individuals. Do not misrepresent yourself.

D. Do not harm the integrity of the Covered Entity's computer systems and networks.

1. Today's information technology is a shared resource. Respect the needs of others when using computer and network resources. Do not tamper with facilities and avoid any actions that interfere with the normal operations of computers, networks, and facilities.

2. Avoid excessive use of computer resources. They are finite and others deserve their share. Chain mail, junk mail, and similar inappropriate uses of Covered Entity resources are not acceptable. Web pages that are accessed to an excessive degree can be a drain on computer resources and, except where significant to the Covered Entity's mission, may require the Covered Entity to ask that they be moved to a private Internet provider.

3. Although a respect for privacy is fundamental to the Covered Entity's policies, understand that almost any information can in principle be read or copied; that some user information is maintained in system logs as a part of responsible computer system maintenance; that the Covered Entity must reserve the right to examine computer files, and that, in rare circumstances, the Covered Entity may be compelled by law or policy to examine even personal and confidential information maintained on Covered Entity computing facilities.

4. You are granted privileges and responsibilities with your account. While these vary between groups, the use of Covered Entity resources for personal commercial gain or for partisan political purposes is inappropriate and possibly illegal.

5. Individual Covered Entity computer systems have varying resources and demands. Some have additional and sometimes more restrictive guidelines applicable to their own user.

Implementation

1. All Covered Entity codes of conduct apply to information technology as well as to other forms of communication and activity.
2. The Region's Privacy and Security Officers and the County IT personnel or contractor who manage County equipment and software may be empowered to suspend some or all privileges associated with computer use in cases of misuse or threat to the integrity of all or part of the Covered Entity's information management resources.
3. Before any permanent action is taken against a user, the user will be advised of the basis for the proposed action and given an opportunity to respond. Concerns about such actions may be raised through the usual administrative channels associated with the County in question.
4. Where a violation of Covered Entity policies or applicable law appears to warrant action beyond a suspension or elimination of computer privileges, the matter shall be referred to the appropriate County for disciplinary action based on recommendations of the Covered Entity. Complaints or concerns about another's use of Covered Entity computer resources should be directed to the Region's Privacy or Security Officer or the County IT personnel or contractor who manage County equipment and software.

SERVER, WORKSTATION, AND MOBILE SYSTEMS SECURITY POLICY

I. POLICY

Covered Entity 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)
- Workstation Use Policy

IV. PROCEDURES

1) General Security Requirements. 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) Desktop System Security Requirements

a) Each Coordinator of Disability Services 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.

b) The system administrator or root account must be password protected.

c) A user identification and password authentication mechanism must be implemented to control user access to the system.

d) A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

e) A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date.

f) All unused or unnecessary services must be disabled.

g) Desktop systems that are located in open, common, or otherwise insecure areas must also implement the following measures:

   i. An inactivity timer or automatic logoff mechanism must be implemented.

   ii. The workstation screen or display must be situated in a manner that prohibits unauthorized viewing.

3) Mobile Systems Security Policy

a) Each Coordinator of Disability Services 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.

b) The system administrator or root account must be password protected.

c) A user identification and password authentication mechanism must be implemented to control user access to the system. All mobile devices and laptops must use a boot password to ensure that the system is only accessible to authorized users.

d) A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

e) A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up-to-date.

f) All unused or unnecessary services must be disabled.

g) Mobile stations that are located or used in open, common, or otherwise insecure areas must also implement the following measures:

i. A theft deterrent device such as a laptop locking cable must be utilized when the device is unattended.
ii. An inactivity timer or automatic logoff mechanism must be implemented.
iii. Reasonable safeguards must be in place to prohibit unauthorized entities from viewing confidential information.

h) Each mobile system that is used to access, transmit, receive, or store ePHI must comply with as many of the aforementioned measures as is allowed by the system and operating system architecture.

PHYSICAL SAFEGUARDS DEVICE AND MEDIA CONTROLS POLICY

I. POLICY

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

II. PURPOSE

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

This policy outlines the policy and procedures 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.

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. PROCEDURES

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.

2) Destruction of Storage Devices or Removable Media

a) Prior to destroying or disposing of any storage device or removable media, care must be taken to ensure that the device or media does not contain ePHI.

b) If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to disposal.

c) If the device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal.

d) In the event ePHI is disposed of, it shall be disposed destroyed in a manner approved of by the Secretary.

3) Reuse of Storage Devices or Removable Media

a) Prior to making storage devices and removable media available for reuse, care must be taken to ensure that the device or media does not contain ePHI.
b) If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to reuse.
c) If the device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to reuse.
d) If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, the use of a data destruction tool between uses is not necessary.

4) Movement of Equipment Housing EPHI

a) Covered Entity shall develop a procedure to determine when an exact retrievable copy of ePHI is required prior to the movement of equipment storing such ePHI.
b) The use of removable media, such as thumb drives, to store or transport ePHI shall be prohibited.

ACCESS CONTROL POLICY

I. POLICY

With respect to systems, applications or networks that Covered Entity controls, Covered Entity will assign a unique name and/or number to each employee performing administrative functions on behalf of Covered Entity that is authorized to access ePHI and will maintain a user authentication procedure.

Covered Entity 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
- Workstation Use Policy
- Server, Desktop, and Wireless Computer System Security Policy

IV. PROCEDURES

1) **Unique User Identification**. To uniquely identify and track one user or workforce member from all others, for the purpose of access control to all networks, systems, and applications that contain ePHI, and the monitoring of access to the aforementioned networks, systems, and applications, the following procedures must be implemented:

a) Any user or workforce member who requires access to any network, system, or application that accesses, transmits, receives, or stores ePHI, must be provided with a unique User Identification string.

b) When requesting access to any network, system, or application that accesses, transmits, receives, or stores ePHI, a user or

workforce member must supply their previously assigned unique User Identification in conjunction with a secure password to gain access to the aforementioned networks, systems, or applications.

c) Users or workforce members must not allow another user or workforce member to use their unique User Identification or Password.

d) Users or workforce members must ensure that their Password is not documented, written, or otherwise exposed in an insecure manner unless it is to be hard coded into the system in which case it will be shared with the appropriate IT personnel.

2) **Firewall Use**. All networks controlled by Covered Entity housing ePHI repositories must be appropriately secured. To ensure that all networks that contain ePHI-based systems and applications are appropriately secured, the following policies and procedures are followed:

a) Networks containing ePHI-based systems and applications must implement perimeter security and access control with a firewall.

b) Firewalls must be configured to support the following minimum requirements:

i. Limit network access to only authorized workforce members and entities.

ii. Limit network access to only legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.

iii. Console and other management ports must be appropriately secured or disabled.

iv. Implement mechanism to log failed access attempts.

v. Must be located in a physically secure environment.

c) The configuration of firewalls used to protect networks containing ePHI-based systems and applications must be documented internally by the Security Officer. This documentation should include a configuration plan that outlines and explains the firewall rules.

3) **Wireless Access**. To ensure that all networks that contain ePHI-based systems and applications are appropriately secured, the following wireless access policies and procedures must be followed:

a) Wireless access to networks containing ePHI-based systems and applications is permitted so long as the following security measures have been implemented:

i. Encryption must be enabled.
ii. MAC-based or User ID/Password authentication must be enabled.
iii. All console and other management interfaces have been appropriately secured or disabled.

b) Unmanaged, ad-hoc, or rogue wireless access points are not permitted on any secure network containing ePHI-based systems and applications.

c) All wireless LANs do not utilize standard 2.4 GHz, 5.0 GHz or microwave radio frequencies. Wireless LANs and devices may utilize infrared frequencies and may not support the typical wireless LAN encryption and security mechanisms. For instance, the use of infrared ports on PDAs, laptops, and printers to transmit ePHI may not allow encryption of that data stream. This is a low risk concern because this implementation of infrared is very short distance and low power.

4) **Remote Access**. To ensure that all networks that contain ePHI-based systems and applications are appropriately secured, the following remote access policies and procedures must be followed:

a) Dial-up connections directly into secure networks are considered to be secure connections and do not require a VPN connection.

b) Authentication and encryption mechanisms are required for all remote access sessions to networks containing ePHI via an Internet service provider or dial-up connection. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, etc.

c) The following security measures must be implemented for any remote access connection into a secure network containing ePHI:

i. Mechanisms to bypass authorized remote access mechanisms are strictly prohibited.
ii. Remote access systems must employ a mechanism to "clear out" cache and other session information upon termination of session.

iii. Remote access workstations must employ a virus detection and protection mechanism.
iv. Users of remote workstations must comply with the HIPAA Security Workstation Use Policy.

d) VPN split-tunneling is not permitted for connections originating from outside the Covered Entity network or from an insecure network within the Covered Entity domain.
e) The workforce member requesting remote access to a secure network containing ePHI-based systems and applications must ensure that the remote workstation device being used by said workforce member meets the security measures detailed in the HIPAA Security Server, Desktop, and Wireless Computer System Security Policy. The owner of the secure network must ensure that the previous requirement has been satisfied before access is granted.
f) The Security Officer in cooperation with the Coordinator of Disability Services shall establish a formal, documented procedure to ensure that remote workstations and mobile devices used by their workforce members to remotely access secure networks containing ePHI-based systems and applications continue to meet the security measures detailed in the Server, Desktop, and Wireless Computer System Security Policy.

5. Automatic Logoff. To ensure that access to all servers and workstations that access, transmit, receive, or store ePHI is appropriately controlled, the following procedures must be followed:

a) Servers, workstations, or other computer systems containing ePHI repositories must employ inactivity timers or automatic logoff mechanisms. The aforementioned systems must terminate a user session after a period of inactivity.
b) Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas, that access, transmit, receive, or store ePHI must employ inactivity timers or automatic logoff mechanisms. (i.e., Password protected screen saver that blacks out screen activity.)
c) Applications and databases using ePHI, such as Electronic Medical Records (EMR), must employ inactivity timers or automatic session logoff mechanisms.
d) If a system requires the use of an inactivity timer or automatic logoff mechanism as detailed in the aforementioned procedures, but does not support an inactivity timer or automatic logoff

mechanism, one of the following procedures must be implemented:

i. The system must be upgraded or moved to support the minimum HIPAA Security Automatic Logoff procedures.
ii. The system must be moved into a secure environment.
iii. All ePHI must be removed and relocated to a system that supports the minimum HIPAA Security Automatic Logoff procedures.

e) When leaving a server, workstation, or other computer system unattended, workforce members must lock or activate the system's Automatic Logoff Mechanism or logout of all applications and database systems containing ePHI.

6. It is expected that System and Security Administrators will configure the system to ensure that:

a) Passwords include security control features to prevent hacking, such as randomization, required password structure (upper and lower case; numbers and letters), non-commonality with personal information, etc.

b) Users change their passwords in accordance with the Password Management Policy.

c) A user ID locks after failed log-in attempts in accordance with the Unique User Identification Policy.

d) The Access Control List is subject to access protection or one-way encryption.

TECHNICAL SAFEGUARDS AUDIT CONTROLS POLICY

I. POLICY

For the systems, applications and networks that Covered Entity controls, with the exception of emails, Covered Entity 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 the Covered Entity, 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)
- General Information System Activity Review Policy

IV. PROCEDURES

1) Audit Control Mechanisms

a) The Security Officer with systems containing medium and high risk ePHI must utilize a mechanism to log and store system activity.
b) Each system's audit log must include, but is not limited to, User ID, Login Date/Time, and Activity Time. Audit logs may include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.
c) System audit logs must be reviewed on a regular basis.
d) Implementation of an audit control mechanism for systems containing low risk ePHI is not required.

2) Audit Control and Review Plan

a) An Audit Control and Review Plan must be developed by the Security Officer. The plan must include:

i. Systems and applications to be logged
ii. Information to be logged for each system
iii. Log-in reports for each system
iv. Procedures to review all audit logs and activity reports

INTEGRITY AND AUTHENTICATION POLICY

I. POLICY

Covered Entity will review whether ePHI maintained on Covered Entity's systems has been altered or destroyed in an unauthorized manner. Covered Entity 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 Covered Entity'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
- HIPAA Security Transmission Policy

IV. PROCEDURES

1) The following mechanisms will ensure the Covered Entity

   a) A mechanism to corroborate that ePHI is not altered or destroyed in an unauthorized manner.
   b) A mechanism for all systems containing ePHI to ensure that ePHI has not been altered or destroyed by a virus or other malicious code.
   c) Error-correcting memory and storage mechanism to authenticate data storage and retrieval.

2) ePHI is backed up in accordance with the Data Back Up Plan Policy.

3) Covered Entity will train members of its workforce not to alter or destroy ePHI in an unauthorized manner.

4) In monitoring use of ePHI, Covered Entity will review and respond to any indication of alteration.

5) For high risk ePHI, a DES (Digital Encryption Standard) encryption mechanism or data checksum can be used to ensure the integrity of data at rest. The use of data authentication mechanisms other than virus detection is not required for low risk ePHI.

PERSON OR ENTITY AUTHENTICATION POLICY

I. POLICY

For the systems, applications and networks that Covered Entity controls, i.e., Microsoft Office 365 and SharePoint, Covered Entity 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. This Policy covers the procedures to be implemented by the Covered Entity's Security Officer 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)
- Unique User Identification Policy
- Password Management Policy

IV. PROCEDURES

1) Covered Entity will review ePHI access on a monthly basis.

2) The persons and entities authorized to access ePHI are listed in the Access Control List, as set out in the Unique User Identification Policy.

3) Workforce members seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity, all in accordance with the applicable policies adopted by Covered Entity.

4) Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information.

5) Workforce members are not permitted to allow other persons or entities to use their unique User ID and password or other authentication information.

6) A reasonable effort must be made to verify the identity of the receiving person or entity prior to transmitting ePHI.

7) It is expected that System and Security administrators will configure the system to ensure that:

a) Passwords include security control features to prevent hacking, such as randomization, required password structure (upper and lower case; numbers and letters), non-commonality with personal information, etc.
b) Users change their passwords in accordance with the Password Management Policy.
c) A user ID locks after failed log-in attempts in accordance with the Unique User Identification Policy.
d) The Access Control List is subject to access protection or one-way encryption.

TECHNICAL SAFEGUARDS TRANSMISSION SECURITY POLICY

I. POLICY

Covered Entity 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)

IV. PROCEDURES

1) EPHI Transmissions to Non- Covered Entity Entities

a) To appropriately guard against unauthorized access to or modification of ePHI that is being transmitted from the Covered Entity domains to a network outside of such networks, the procedures outlined in this Paragraph must be implemented.

b) All transmissions of ePHI from the Covered Entity domains to a network outside of the aforementioned networks must utilize an encryption mechanism between the sending and receiving entities or the file, document, or folder containing said ePHI must be encrypted before transmission or must be password protected.

c) All transmissions of ePHI from the Covered Entity domains to a network outside of the aforementioned networks should include only the minimum amount of ePHI.

d) For transmission of ePHI from the Covered Entity domains to a network outside of the aforementioned networks utilizing an email or messaging system, see Paragraph 4 below.

2) EPHI Transmission between the Covered Entity Entities

a) When transmitting ePHI over an electronic network between the Covered Entity entities, the ePHI must be password-protected or encrypted before transmission as described below.

b) All transmissions of ePHI from the Covered Entity domain must utilize an encryption mechanism or be password-protected.

c) All transmissions from the Covered Entity that do not contain ePHI require no additional security mechanisms.

3) EPHI Transmissions Using Electronic Removable Media

Transmissions using Electronic Removable Media shall be prohibited.

4) EPHI Transmissions Using Email or Messaging Systems

a) The transmission of ePHI from the Covered Entity to a client via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

i. The client has been made fully aware of the risks associated with transmitting ePHI via email or messaging systems.
ii. The client has formally, in writing or through email, authorized the Covered Entity to utilize an email or messaging system to transmit ePHI to them.
iii. The client's identity has been authenticated.
iv. The email or message contains no excessive history or attachments.

b) The transmission of ePHI from the Covered Entity to an outside entity via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

i. The receiving entity has been authenticated.
ii. The receiving entity is aware of the transmission and is ready to receive it.
iii. The sender and receiver are able to implement a compatible encryption mechanism or password.
iv. All attachments containing ePHI are encrypted or password-protected.

c) The transmission of ePHI within the Covered Entity via an email or messaging system is permitted without additional security measures or safeguards so long as only a minimal amount of ePHI is being transmitted and the ePHI is not high risk, sensitive or critical. ePHI that is high risk, sensitive or critical should not be sent through clear text email; such ePHI should be sent via encrypted attachment or other secure measure as described in paragraph 4(b) above. If an email or message includes an

attachment that contains ePHI, the attachment must be encrypted or password-protected before transmission.

d) The transmission of all emails pertaining to the business of the Covered Entity or containing ePHI between members of the Covered Entity's workforce must be sent by use of the Covered Entity's Microsoft Office 365 email system.

e) Email accounts that are used to send or receive ePHI must not be forwarded to non- Covered Entity accounts.

5) EPHI Transmissions Using Wireless Network Systems

a) The transmission of ePHI over a wireless network within the Covered Entity domains is permitted if the following conditions are met:

i. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized.
ii. The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network.

b) If transmitting ePHI over a wireless network that is not utilizing an authentication and encryption mechanism, the ePHI must be encrypted before transmission.

c) The authentication and encryption security mechanisms implemented on wireless networks within the Covered Entity domains are only effective within those networks. When transmitting outside of those wireless networks, additional and appropriate security measures must be implemented in accordance with this Policy.

6) Additional Requirements

a) When transmitting ePHI electronically, regardless of the transmission system being used, Workforce members must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the ePHI requested.

b) If the ePHI being transmitted is not to be used for treatment, payment or health care operations, only the minimum required amount of PHI should be transmitted.

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 or business associate 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 section 264 of Pub. L. 104-191, , or sections 13400-13424 of Pub. L. 111-5, 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, Covered Entity, 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, (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plain; or (3) 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).

Family member means, with respect to an individual, a dependent (as defined in 45 CFR 144.103) of the individual, or any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. This includes relatives by affinity (such as by marriage or adoption) and relatives by less than full consanguinity (such as half-siblings).

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; patient safety 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, enrollment, 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 45 CFR 164.105(a)(2)(iii)(D).

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

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.

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.

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 45 CFR part 164, 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 45 CFR 164.512(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 and court-ordered warrants; subpoenas issued 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, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

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) Health care electronic funds transfers (EFT) and remittance advice.
(12) 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.

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.