Liberty Healthcare Corporation
THE FREEDOM TO SUCCEED™

Liberty QualityCare®
Liberty Healthcare Corporation Standard Operating Procedures

Title:	**Introduction to HIPAA Privacy and Security Program**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	**01/23/2018**
Functional Area:	**Administration**		

INTRODUCTION

Liberty Healthcare Corporation, Liberty of Indiana Corporation, Liberty of Oklahoma, Liberty Behavioral Health ("Liberty Healthcare Corporation and Its Affiliates - Liberty") has various operations for health care providers and health plans which make it a "business associate" as defined by HIPAA.

In the course of its day to day operations, Liberty uses and discloses protected health information of covered entity clients. In recognition of its obligation to protect patient information, Liberty protects the confidentiality, availability, integrity and privacy of protected health information in accordance with federal and state law, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the "HIPAA Regulations" (45 C.F.R. Parts 160 & 164, as currently drafted and subsequently updated or amended) and the amendments in Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), as Title XIII of Division A and Title IV of Division B of the American Reinvestment and Recovery Act of 2009 and subsequent regulation (collectively "HIPAA").

In compliance with HIPAA requirements and state laws, certain contract provisions agreed to between Liberty and its covered entity clients with respect to the confidentiality of PHI are passed through to applicable subcontractors in their contracts with Liberty.

Liberty uses and discloses protected health information on behalf of its covered entity clients as a business associate to provide services for those clients. Liberty uses and discloses protected health information on behalf of clients for payment and health care operations purposes. Liberty also may use and disclose protected health information for treatment on behalf of covered entity clients, but does not submit any health information in standard electronic form in connection with HIPAA covered transaction. Only those providers who submit the specified standard transactions in 45 C.F.R. Part 162 (for claims payment, eligibility status, etc.) are considered HIPAA covered entities.

DEFINITIONS

1. A "Liberty Subcontractor" is a person or entity to whom Liberty as a Business Associate delegates a function, activity, or service other than in the capacity of a member of the Workforce of such Business Associate. Liberty has Subcontractors that assist Liberty in performing tasks. All Liberty Subcontractors are required to execute a Business Associate Agreement. From time to time a Liberty Subcontractor may also be called a "Business Associate".
2. A "Business Associate" is a person or entity that creates, receives, maintains or transmits health information on behalf of a covered entity for a function or activity that is regulated by HIPAA (Id.) Liberty acts as a business associate for many of its clients, who are often covered entities, when engaging in day-to-day operations.
3. A" Designated Record Set" means: (1.) A group of records maintained by or for a covered entity that is (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims, adjudication , and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals (45 C.F.R. 164.501). The term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity (45 C.F.R. 164.501).

4. The Privacy Rule and the Security Rule are together designed to maintain the confidentiality, integrity and availability of "protected health information," (45 C.F.R. 160.103) frequently referred to as "PHI". "Health Information" is information that is created or received by a covered entity or employer relating to the past, present or future physical or mental health or condition of an individual, or the provision of health care to the individual, or to the past, present or future payment for the provision of health care to the individual. "Protected Health Information" (PHI) is health information that is or can be associated with a particular individual.

5. The Privacy Rule and the Security Rule apply to the "use" or "disclosure" of PHI. "Use" (45.C.F.R. 164.103).

6. Administrative Simplification is part of the Federal Law for Health Information Privacy and Security was passed by Congress in 1996 as the Health Insurance Portability and Accountability Act ("HIPAA" or the "Act"). The principle thrust of the legislation was to prevent health care fraud and to provide continuity of health insurance for workers who change jobs. As part of the same legislation, an "Administrative Simplification" provision was added to address electronic health care transactions (Public Law 104-191). The goal of Administrative Simplification was to end hundreds of different formats and coding requirements used to process and pay claims. The legislation mandated the adoption of common electronic formats and coding when performing electronically the most common health care transactions. The objective is to encourage efficiencies of converting from cumbersome, time-consuming and labor-intensive paper-based processes to uniform, streamlined electronic transactions. Placing individual information where it can be accessed electronically heightens the risk of unauthorized intrusion into files containing personal information that many people consider private. The push to electronic health care transactions was accompanied by mandates that providers, health plans and clearinghouses adopt security protections and privacy protections to protect the confidentiality, integrity and availability of that information. The HIPAA Privacy Rule (45 C.F.R. Parts 160 and 164) and the Security Rule (45 C.F.R. Parts 160 and 164) are the two (2) sets of regulations with which covered entities and business associates must comply when handling patient information. Regulated entities must also consider a variety of State laws designed to protect individuals relative to data breaches which could compromise personal information. In 2009, Congress passed the American Recovery and Reinvestment Act (ARRA- Public Law 111-115). Title VIII of ARRA, called the Health Information Technology for Economic and Clinical Health Act (HITECH) amended HIPAA in various ways and included federal security breach notification requirements. These requirements were further codified in a Breach Notification Rule (45 C.F.R. – 164.404 et *seq.*). Finally, in January, 2013, the Department of Health and Human Services released several final rule changes to HIPAA; these changes are commonly referred to as the Omnibus Rule. The Omnibus Rule finalized certain requirements from the HITECH Act formalizing the direct responsibilities of business associates as well as several key changes to the Privacy Rules and the Breach Notification Rule

7. Liberty's Workforce - All Liberty employed and physician subcontracted staff.

Regulatory References

45 C.F.R. 160 & 164
45 C.F.R. 162
45 C.F.R. 164.501
45 C.F.R. 160.103
45 C.F.R. 164.103
Public Law 104-191
45 C.F.R. Parts 160 and 164
Public Law 111-115
45 C.F.R. 164.404 *et seq*

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:48:15 -05'00'

Liberty QualityCare®
Liberty Healthcare Corporation
Standard Operating Procedures: INDEX – HIPAA Privacy and Security Plan

Title:	**Index to Liberty Privacy and Security Program**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Introduction to HIPAA Privacy and Security Plan - Brief Overview of the Program

Index HIPAA Standard Operating Procedures (SOPs) – HIPAA Privacy and Security Program 2019

1. HIPAA Rules and Risk Management
2. HIPAA Privacy Officer
3. HIPAA Complaints, Sanction and Non-Retaliation
4. HIPAA Protection, Safeguards and Verification
5. HIPAA Uses & Disclosures and Minimum Necessary
6. HIPAA Authorization Requirements
7. HIPAA Business Associate/Client Agreements
8. HIPAA Right to Request Restrictions and Confidential Communication
9. HIPAA Tracking and Accounting of Disclosures of Protected Health Information
10. HIPAA Right to Request Access to Designated Record Set
11. HIPAA Security Management
12. HIPAA Right to Request an Amendment to Protected Health Information (PHI)
13. HIPAA Security Officer
14. HIPAA Information Access Management
15. HIPAA Workforce Security
16. HIPAA Security Awareness and Training
17. HIPAA Contingency and Disaster Recovery Plan

18. HIPAA Asset Tracking

Index Standard Operating Procedures (SOPs) – HIPAA Privacy and Security Plan 2019

19. HIPAA Data Integrity for Electronic Protected Health Information (ePHI)
20. HIPAA Data/Security Incidents
21. HIPAA Security Evaluation
22. HIPAA Facility Access Controls
23. HIPAA Workstation Use & Security
24. HIPAA Device and Media Controls
25. HIPAA Portable Computing Devices
26. HIPAA Remote Access
27. HIPAA Access Control
28. HIPAA Audit Control
29. HIPAA Person or Entity Authorization
30. HIPAA Transmission Security
31. HIPAA Document Retention and Storage
32. HIPAA Protection from Malicious Software
33. HIPAA Change Control
34. Breach Notification

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:48:34 -05'00'

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #1:
Rules Risk Management Activities

Title:	**HIPAA Rules and Risk Management**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/18/2018**
Location:	**ALL LOCATIONS**	**Last Revision Date:**	**12/18/2018**
Functional Area:	**ADMINISTRATION**		

POLICY

To ensure compliance with the HIPAA regulations, Liberty Healthcare Corporation ("Liberty") shall engage in a variety of activities for HIPAA that are an integral part of the Liberty Compliance Program.

PROCEDURE

Privacy Rule: To ensure compliance with the Privacy Rule, Liberty shall require annual Liberty workforce (Liberty employed and physician subcontracted staff) training in the HIPAA rules and shall develop a complaint process in the Corporate Compliance program to ensure that Liberty's workforce members can file complaints regarding policies, practices, and compliance with HIPAA. The Corporate Compliance Program includes standard operating procedures for disciplinary actions and terminations for Liberty's workforce members who violate this Corporate Compliance Program or HIPAA in order to mitigate damages known to have resulted from Liberty's improper use or disclosure of PHI. Liberty shall annually review the HIPAA Privacy Standard Operating Procedures. Liberty shall maintain all required documentation for its HIPAA Compliance for a period of at least six (6) years from the date of the documents creation or the date it was last in effect, whichever is later (45 C.F.R. 164.530 (j)(2).

Security Rule: Liberty shall establish procedures and mechanisms to protect the confidentiality, integrity and availability of ePHI. Liberty shall implement administrative, physical and technical safeguards to protect ePHI (45 C.F.R 164.306(a)). Liberty shall subcontract with a consultant as a business associate to perform a security risk assessment at our North Carolina Independent Assessment Program which currently has the most significant use of ePHI and the results of this risk profile is a similar survey with a few additions used for all of Liberty's programs across the organization - revised 08/19/2015). Liberty shall annually evaluate the HIPAA Security Standard Operating Procedures in light of existing threats and new technologies. In addition, an annual risk assessment will be performed IF ANY of the operations, processes or systems of Liberty change in a given year. The computer security guidelines issued by the National Institute of Standards and Technology (NIST) shall be the operative guidelines for security standards compliance, and shall be a guide to assist Liberty in its risk assessment. Liberty shall apply appropriate sanctions to Liberty's Workforce members who violate security Standard Operating Procedures SOPs. (45 C.F.R. 164.308(a) (1) (ii) (C).

Breach Notification Rule: In 2009 the HIPAA regulations were amended to include new breach notification requirement (45 C.F.R. 164.400-164.414). The Breach Notification Rule was further amended by the Omnibus Rule in 2013 (78 Federal Regulation 5566). Liberty shall notify individuals, the Secretary of the U.S. Department of Health & Human Services, and in some cases the media, when "unsecured" PHI has been breached. A breach is the unauthorized "access, acquisition, use or disclosure" of PHI. Liberty shall have an explicit Standard Operating Procedure SOP) titled "Data/Security Incidents", which includes suspected or actual breaches of PHI.

State Law: State Preemption under HIPAA: Liberty shall abide by both federal and state laws regarding the privacy and security of PHI. This is a challenge, since each state may protect different types of personal information. The HIPAA regulations have two (2) main rules relating to how they intersect law. FIRST, state laws that are contrary to the HIPAA regulations are preempted by the HIPAA regulations, which mean the HIPAA regulations apply (45 C.F.R. 160.202). SECOND, when a state law is more stringent than the HIPAA regulations, Liberty shall abide by the more stringent

regulation or statute.

State Law: State Data Breach Laws: As of this implementation, forty-six (46) states have state data breach laws that impact any unauthorized disclosure of personally identifiable information by Liberty. If there is a potential breach incident of personal information, but the incident does not meet the definition of unsecured protected health information, the incident shall still be evaluated by Liberty's Vice President,Performance/Corporate Compliance/Privacy Officer, the Senior Vice President/Chief Operating Officer and General Counsel for notification requirements under existing state laws.

Regulatory References

45 C.F.R. 164.530(j)(2)
45 C.F.R. 164.306 (a)
45 C.F.R. 164.308(a)(1)(ii)(C)
45 C.F.R. 164.400-164.414
45 C.F.R. 160.202

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:49:11 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #2: Privacy Officer

Title:	**HIPPA Privacy Officer**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	**12/18/2018**
Functional Area:	**Administration**		

POLICY

Liberty shall assign a Privacy Officer to oversee and implement the Privacy HIPAA program and to ensure Liberty's compliance with the requirements of all privacy requirements, including but not limited to the HIPAA Privacy Rule and other state laws regarding the privacy of personal information. The Privacy Officer shall be responsible for receiving complaints about matters of individual privacy. Liberty's Privacy Officer, in collaboration with the Senior Vice President/Chief Operating Officer and General Counsel, shall respond in a timely manner to additional privacy protections requests or requests from individuals to exercise their individual rights, with careful consideration and respect. Liberty's Privacy Officer shall be responsible for the development and implementation of all Privacy Standard Operating Procedures (SOPs). Liberty's Privacy Officer shall delegate their functions as appropriate.

PROCEDURE

1. Privacy Standard Operating Procedures: Liberty's Privacy Officer shall communicate and implement the Liberty HIPAA Privacy and Corporate Compliance programs.
2. Training: (a) Liberty's Privacy Officer shall have oversight of initial and ongoing HIPAA Privacy Training for all Liberty workforce members that support Liberty operations in the HIPAA Programs. The training program on HIPAA includes awareness of privacy, security and breach notification issues. The training shall also include other federal or state privacy, security and data breach law as determined by Liberty's Privacy and Security Officers. All Liberty workforce members shall participate in the HIPAA Training within a reasonable period of time from beginning work for Liberty, preferably prior to handling any PHI. (b) All new Liberty workforce members (SOP) shall be trained according to the onboarding section of Liberty's SOP "Information Access Management". (c) Liberty shall also utilize the Employee Self Service to both introduce the HIPAA SOPs and to notify the workforce members of changes to these established SOPs. (d) All Liberty workforce members shall have HIPAA Training annually and documentation of this annual training will be retained by Human Resources. (e) Liberty shall ensure that this annual HIPAA training will include information regarding the protection and guarding against and reporting of malicious software as well as HIPAA training regarding SOPs for the creation and protection of passwords.
3. Complaints: Liberty's Privacy Officer shall serve as the individual to receive and investigate complaints. Once the complaint has been evaluated by the Privacy Officer additional aspects of the evaluation and investigation may be delegated. All HIPAA complaints and their disposition will be documented and retained by the Privacy Officer for a minimum of six (6) years.
4. Non Retaliation: In congruence with Liberty's Complaints, Sanction and Non-Retaliation HIPAA Standard Operating Procedure, the Privacy Officer shall ensure that no intimidation, threats, coercion, discrimination or retaliation shall be lodged toward an individual for exercising an individual right or for filing a complaint.
5. Sanctions: In collaboration with the Senior Vice President/Chief Operating Officer, General Counsel, appropriate Liberty Managers, and Supervisors, the Liberty Privacy Officer shall ensure that violations of the HIPAA Program

and any associated SOPs are addressed. The Liberty Privacy Officer shall document any sanctions which are applied, and the documentation shall be retained in the Human Resources section of the personnel file of the employee. If the individual is not a Liberty Employed staff member, the Privacy Officer shall maintain the documentation of the sanction.

6. Review and Revisions to the HIPAA Privacy Standard Operating Procedures (SOPs): The Liberty Privacy Officer shall review the HIPAA SOPs annually and introduce revisions if there are any changes in Operations or changes in the law.
7. Appropriate Safeguards: The Liberty Privacy Officer shall ensure that appropriate administrative, technical, and physical safeguards shall be implemented to protect the confidentiality, integrity and availability of PHI from any intentional or unintentional use or disclosure that is in violation of Liberty's SOPs.
8. Business Associate Agreements: The Liberty Privacy Officer shall be responsible for securing Business Associate/Subcontractor Agreements when necessary to meet the combined requirements of the Privacy Rule and Security Rule – revised 08/20/2015.
9. Documentation Retention: The Liberty Privacy Officer shall ensure that all documentation required for the HIPAA Privacy Program and associated SOPs shall be maintained for a minimum of six (6) years.

Regulatory References

45 C.F.R. 164.530(a)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:51:59 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #3: Complaints, Sanction, and Non-Retaliation

Title:	**HIPAA Complaints, Sanction and Non-Retaliation**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

In recognition of the paramount importance of the privacy and security of protected health information (PHI), Liberty's workforce members shall abide by the HIPAA Privacy and Security Compliance Program. Any violation by a member of the Liberty workforce of the HIPAA Privacy and Security Compliance Program or associated Standard Operating Procedures shall be grounds for disciplinary action up to and including termination of employment or contract termination.

PROCEDURE

1. Anyone who knows or has reason to believe that an individual's privacy or confidentiality has been violated, or another person has violated Liberty's HIPAA Privacy and Security Program shall report the matter promptly to his or her supervisor OR Liberty's Privacy Officer at 610-668-8800 Extension #193 OR call Liberty's Employee Help Line at 1-800-653-7174. If the violation may have resulted in a Breach of Unsecured PHI, Liberty's workforce members shall report the violation to the Security Officer at 610-668-8800 Extension #183.
2. Liberty's Privacy Officer in collaboration with the Senior Vice President/Chief Operating Officer and General Counsel shall respond and investigate all reported complaints that do not include a security rule violation or Security SOP violation and take steps to remedy the situation when appropriate. Any complaints about the security SOPs shall be brought to the attention of Liberty's Security Officer for investigation and response.
3. Whenever possible, Liberty's Privacy Officer shall make every effort to handle the reported matter confidentially.
4. Liberty shall not intimidate, threaten, coerce, discriminate against or take any retaliatory action against any individual for voicing a concern or complaint. Any attempt to retaliate against a person reporting a violation of the HIPAA Privacy and Security Program will itself be considered a violation of this Standard Operating Procedure that may result in disciplinary action up to and including termination of employment or contract termination with Liberty.
5. Upon conclusion of the investigation, Liberty's Privacy Officer or Security Officer shall prepare a written report with findings and conclusions that have been reviewed with Liberty's Senior Vice President/Chief Operating Officer and General Counsel. If employee discipline is recommended, these collaborative findings and conclusions will be sent to Liberty's Vice President of Human Resources. The Vice President of Human Resources in collaboration with General Counsel will make the final determination of the appropriate disciplinary action or contract action based upon the written report.

SAMPLE Of POSSIBLE Disciplinary/Contract Modification Matrix – All final disciplinary actions are made collaboratively by the Vice President of Human Resources and General Counsel

Level and Definition of Violation	**Example of Violation**	**Action Steps**
Accidental and/or due to lack of clarity	Improper disposal of PHI Improper protection of records i.e. leaving information unattended on a desk First Offenses	Re-Training on HIPAA Oral Warning with documented discussion of Standard Operating Procedures and requirements
Purposeful violation of privacy or an unacceptable number of previous violations	Accessing or using PHI without having a legitimate need to do so Not forwarding appropriate information or requests to Liberty's Privacy Officer for processing	Re- Training on HIPAA Written warning with documented discussion of Standard Operating Procedures and requirements Potential Termination of Employment or Contract Termination
Purposeful violation of privacy Standard Operating Procedures with associated potential for individual harm	Disclosure of PHI to unauthorized individual or company Sale of PHI to any source Any uses or disclosures that could invoke harm to an individual	Termination of Employment or Contract Termination
Multiple violations	Repeated occurrences of any of the above examples or other violations	Any sanction described above, up to and including termination of employment or contract termination

Regulatory References

45 C.F.R. 164.308(a)(1)(ii)(C)
45 C.F.R. 164.502
45 C.F.R. 164.530(d)
45 C.F.R. 164.530(g)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:53:20 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #4: Protection, Safeguards and Verification

Title:	**HIPAA Protection, Safeguards, and Verification**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	**01/18/2016**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall identify the PHI it maintains and it shall institute the following protections to ensure the information is not used or disclosed for any purposes other than those purposes permitted by law.

PROCEDURE

Printed and Hard Copy documentation:

1. Designation of Liberty's workforce members with access to PHI and direct all incoming documentation, generally either US mail or interoffice mail.
2. Liberty implemented a "clean desk" practice so that all PHI shall be put away each time Liberty's workforce members are away from his/her desk and shall be placed in locked drawers or cabinets at the end of each work day and when the Liberty workforce member leaves their office.
3. PHI in paper format will be destroyed by shredding following a period of six (6) years from the date of the document creation or the date it was last in effect whichever is later.

E-mail and electronic storage:

4. All PHI in emails shall be limited to the minimum necessary (i.e. refrain from forwarding string emails containing PHI; instead create new messages which limit the PHI and the recipients of the email).
5. Emails containing PHI shall be encrypted. If the encryption tool is not operational for a particular Liberty entity or program, then password protection of emails with PHI shall be utilized.
6. Liberty's workforce members shall only access the email system after a password entry.
7. Follow Liberty's HIPAA Privacy and Security Standard Operating Procedures as a part of this HIPAA Program to address Security rule requirements.
8. Emails with PHI shall only be sent from a Liberty provided account.
9. Text messages shall never include PHI.

Facsimiles

10. All faxes are routed to Liberty's workforce member's email system and shall be handled just as any other email containing PHI as described herein.
11. **Before sending outgoing faxes containing PHI, confirm that the fax number is correct. JAS01/18/2016**

Oral Communication

12. All oral conversations shall be limited in content in conformance with the Minimum necessary standard.
13. All conversations shall be made with authorized individuals.
14. If conversation cannot be reasonably made private or not overheard, Liberty's workforce members shall refrain from holding the conversation until it can be moved to a secure location. Speaker phone shall not be used under any circumstances, except if there is a closed door in the office.
15. Voicemail messages shall only be used when necessary and should not contain PHI.

Verification

16. Liberty shall ensure that it reasonably determines the identification and authority of any individual requesting PHI. In general, Liberty shall interface only with covered entity and business associate clients seeking protected health information. If at any time Liberty's workforce member verifying the information is uncomfortable or suspects there is an issue, the verification shall be escalated to their supervisor.
17. If an individual requests protected health information and has not previously been identified as a Liberty workforce member or vendor of the covered entity, the identity and authority of such individual shall be established and, if necessary approved by the Privacy Officer prior to the disclosure of any protected health information.
18. Liberty generally does not need to disclose protected health information to personal representatives or executors of estates. If such a request is made it shall be sent to the Privacy Officer and General Counsel for a determination.

Regulatory References

45 C.F.R. 164.514(h)
45 C.F.R. 164.530

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:53:59 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #5:
Uses & Disclosures and Minimum Necessary Standard

Title:	**HIPAA Uses & Disclosures and Minimum Necessary Standard**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall limit its uses and disclosures of protected health information (PHI). Liberty shall require that for routine activities performed by Liberty workforce members, the least amount of PHI shall be used, requested or disclosed. To the extent possible the least amount of PHI shall be a "limited data set". A "limited data set" is a limited set of identifiable patient information as defined in the Privacy Regulations 45 C.F.R. 164.514(e) (2) and the purpose of the disclosure shall only be for research, public health or health care operations. As a vast majority of Liberty's workforce uses and disclosures make it impracticable to utilize a "limited data set", this Standard Operating Procedure (SOP) still shall require that the use, request or disclosure involve the least amount of PHI necessary to accomplish the intended purpose of the use, request, or disclosure, whenever possible.

PROCEDURE

1. Questions regarding non-routine uses, disclosures or requests for PHI shall immediately be directed to Liberty's Privacy Officer, who will make determinations regarding the non-routine use, disclosure or request on a case by case basis.
2. When Liberty's workforce members provide treatment on behalf of Liberty's covered entity clients, they are permitted to use and disclose PHI without being restricted by the minimum necessary SOP. This would not include any activities performed by administrative staff.
3. Liberty's workforce members may use and disclose PHI without being restricted by the minimum necessary for the purpose of payment and healthcare operations. This includes but is not limited to: insurance enrollment, disenrollment, eligibility determinations, claims payments, subrogation activities, appeals of adverse benefit determinations, client service and informing members of the health-related benefit options, data analysis, including but not limited to underwriting, renewing or replacing health insurance benefits or carriers, benefit plan design and health care operations within the meaning of HIPAA regulations .
4. Liberty's workforce members shall also be required or requested to use or disclose PHI for the following reasons: Following consultation with Liberty's General Counsel, (1) when it is required by federal, state or local law ; (2) for public health activities to a public health authority that is authorized to collect or receive such information for the purpose of preventing or controlling disease or injury; (3) to a public authority regarding child abuse or neglect; (4) to someone subject to the jurisdiction of the Food and Drug Administration regarding regulated food or drug products; (5) to a person who may have been exposed to a communicable disease if such communications are authorized by law and when requested by subpoena or other legal document, to avert serious threat to public health or safety.
5. Liberty shall be required or requested to use or disclose PHI for specialized government functions. General Counsel shall be consulted if this use or disclose of PHI involved (1) the military, veterans activities, security and intelligence; (2) protective services for the President and others; (3) State Department of the United States; (4) correctional institutions; (5) other law enforcement custodial situations; (6) and covered entities under HIPAA that are part of a governmental program providing public benefits.

6. Liberty shall disclose protected health information to the extent necessary for workers compensation or other similar programs as established by law.
7. Liberty shall NOT use or disclose PHI for fundraising purposes. However, in the event that one of Liberty's covered entity clients requests that Liberty send a fundraising communication on its behalf, Liberty will comply with the covered entity client's Notice of Privacy Practices, as well as any opt-out methods provided by the covered entity client, consistent with limitations on such disclosures in the Privacy Rule.
8. Liberty may disclose PHI to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual if the correctional institution or law enforcement officer represents that the PHI is necessary for: (1) the provision of health care to the individual; (2) the health and safety of that individual and other inmates; (3) the health and safety of the officers, employees, or others at the correctional institution; (4) law enforcement on the premises of the correctional institution; (5) or the administration and maintenance of the safety, security, and good order of the correctional institution.
9. Liberty's SOP shall require that on a routine basis, the least amount of PHI shall be used, requested, or disclosed**.** To the extent practical, the least amount of PHI shall be limited to a "limited data set." If a limited data set is used, a data use agreement may be utilized instead of a business associate agreement if authorized by Liberty's Privacy Officer. A "limited data set" is PHI that does not include the following direct identifiers of the individual, relatives, employers or household members of the individual to whom the PHI concerns:
    - Names
    - Postal address information, other than town or city, State and zip code
    - Telephone numbers
    - Fax numbers
    - Electronic mail addresses
    - Social Security numbers
    - Medical record numbers
    - Health plan beneficiary numbers
    - Account numbers
    - Certificate/license numbers
    - Vehicle identifiers and serial numbers, including license plate numbers
    - Device identifiers and serial numbers
    - Web Universal Resource Locators (URLs)
    - Internet Protocol (IP) address numbers
    - Biometric identifiers, including finger and voice prints
    - Full face photographic images and any comparable image
10. If the nature of the use, request or disclosure makes it impracticable to utilize a "limited data set", this SOP shall require that the use, request, or disclosure involve the least amount of PHI necessary to accomplish the intended purpose of the use, request, or disclosure.
11. Business Associates of Liberty Healthcare Corporation (Liberty) shall be required by contract (Business Associate Agreement) to limit uses and disclosures to those permitted by law and contract and to limit all uses and disclosures to the minimum necessary.

Regulatory References

45 C.F.R. 164.514(e)(2)
45 C.F.R. 164.502(b)
45 C.F.R. 164.508
45 C.F.R 164.512
45 C.F.R. 164.514(f)
45 C.R.R. 164.501

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:55:01 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #6: Authorization Requirements

Title:	**HIPAA - Authorization Requirements**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall ensure that a valid authorization shall be obtained, by either Liberty as the covered entity or its covered entity client, prior to any use or disclosure of PHI for a purpose other than those described in Standard Operating Procedure (SOP), "HIPAA USES AND DISCLOSURES AND MINIMUM NECESSARY", including marketing or sale of PHI.

PROCEDURE

1. If Liberty uses or discloses PHI for any purpose other than those described in SOP – "HIPAA Uses and Disclosures and Minimum Necessary", Liberty shall obtain a HIPAA- compliant authorization – 'Authorization to Use or Disclose Protected Health Information' which can be found attached to this SOP.
2. As noted on the Authorization attached to this Standard Operating Procedure, Liberty shall not condition the provision to an individual for treatment or payment on the provision of an authorization.
3. Liberty shall obtain a valid authorization to use or disclose PHI for its own or a covered entity client's marketing purposes, as defined under HIPAA (45 C.F.R. 16.508(3). If Liberty uses or discloses PHI for marketing that involves direct or indirect payment from a third party, the authorization from the individual shall state that payment is involved in order to be valid. Any use or disclosure of PHI by Liberty for marketing purposes shall also be in compliance with any applicable business associate agreements.
4. Liberty shall obtain a valid authorization before engaging in any sale of PHI. An authorization for sale of PHI must state that Liberty Healthcare Corporation (Liberty) is receiving payment for the disclosure. Liberty shall also comply with any applicable business associate agreement obligations if engaging in the sale of PHI.

Regulatory References

45 C.F.R. 164.508(c)
45 C.F.R. 164.501
45 C.F.R. 164.508

See PHI Authorization under Forms on the Shared Drive

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:55:41 -05'00'

Return to Index

Authorization to Use or Disclose Protected Health Information

Once completed the attached authorization to release records permits Liberty Healthcare Corporation and Its Affiliates (Liberty) OR its designee to disclose records in accordance with the authorization as provided herein.

Name: _____

Address: _____

Date of Birth: _____

All sections must be completed.

Section A. Health Information to be Used and/or Disclosed

Health information to be released and /or used, including (if applicable) the time period(s) to which the information relates. Select ONLY ONE of the following:

☐ All of my past, present or future health claims and/or medical records maintained by Liberty Healthcare Corporation.

☐ All of my health information relating to Claim # _____ OR Date of Service _____

☐ Other (MUST specify) _____

Section B. Person(s) Authorized to Use and/or Receive Information

Specify the person(s) or class of people authorized to use and/or receive information described in Section A

_____

Section C. Purposes for which information will be Used and/or Disclosed

☐ To facilitate the resolution of a claims dispute

☐ Other (MUST specify) _____

Section D. Expiration of Authorization

Specify when this Authorization expires (Provide a date or Other – Triggering Event)

☐ On the following date: _____

☐ OTHER – Triggering Event: _____

I understand that the information disclosed above may be re-disclosed to additional parties and no longer protected for reasons beyond the control of Liberty Healthcare Corporation and Its Affiliates (Liberty).

I believe that I have the right to:

1. **Revoke this authorization at any time by sending written notice to: Liberty Healthcare Corporation and Its Affiliates (Liberty). I am aware that such a revocation will not affect Liberty Healthcare Corporation and Its Affiliates (Liberty's) prior reliance on the uses or disclosures pursuant to this organization.**
2. **Inspect a copy of Protected Health Information being used or disclosed under federal law.**
3. **Receive another copy of this authorization.**

I also understand that if I do not sign this document, it will not condition my treatment, payment, enrollment in a health plan, or eligibility for benefits whether or not I provide authorization to use or disclose protected health information.

_____ _____

Signature of Individual or Individual's Authorized Representative **Date:**

Approved By: _____

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #7:
Business Associate/Client Agreements

Title:	**HIPAA Business Associate/Client Agreements**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**Administration**		

POLICY

All of Liberty Healthcare Corporation (Liberty) subcontractors and vendors shall have an executed business associate agreement as required by law. To the extent that Liberty is considered a business associate, Liberty shall execute the appropriate document. For the purposes of this Standard Operating Procedure (SOP), "Business Associate" means a person or entity who is not a Liberty employed staff member , including a "Liberty subcontracted staff or another subcontractor" (means a person or entity, other than a Liberty employed staff , to whom a business associate delegates functions or activities), who creates, receives, maintains or transmits PHI for functions or activities regulated by the HIPAA Privacy Rule on behalf of Liberty including but not limited to , the following functions: claims processing or administration, utilization review, quality assurance, billing, benefit management, and re-pricing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, or financial services.

PROCEDURE

I. Business Associates (Subcontractors)

1. Liberty shall require all business associates to have a current business associate agreement with Liberty prior to permitting the use or disclosure of PHI by or to the subcontractor or the business associate.
2. Liberty shall require a business associate agreement with any covered entity before Liberty uses or discloses PHI on behalf of or to the covered entity.
3. Prior to entering into any service contract, Liberty shall identify and determine whether the service provider is a business associate. In case of a question as to whether a business associate agreement is necessary, Liberty's Privacy Officer shall be consulted.
4. Liberty's Privacy Officer shall maintain a "standard" business associate agreement that shall be presented to service providers and contractors who shall or may have the potential to access any PHI. There may be different "standards" for different relationships. The "standard" shall maintain all required terms and conditions outlined in #6 below. As the "standard" may change from time to time, it is not attached to this SOP but a copy is maintained in a locked cabinet in Liberty's Privacy Officer's locked office.
5. The business associate shall either (a) be provided with Liberty's standard business associate agreement or (b) provides a copy to Liberty of their standard business associate agreement. If a modification is made to Liberty's standard agreement or Liberty is asked to execute the business associate's standard business associate agreement, the documents will be referred to the Privacy Officer for review and response.
6. All business agreements shall have, at a minimum each on the following clauses: (1) A description of the uses and disclosures of PHI permitted and required by the services agreement and the business associate agreement;(2) a prohibition on further uses and disclosures except that the business associate may (a) use or disclose PHI for the proper management and administration of the business associate; (b) provide data aggregation services. (3) Provisions that address: (a) No further uses or disclosures other than as permitted or required by law, the services agreement or the business associate agreement; (b) The use of appropriate safeguards to prevent the use or

disclosure of PHI other than as provided by the business associate agreement;(c) The reporting of any uses or disclosures not provided for by the business associate agreement of which the business associate is aware; (d) Ensure that any agents or subcontractors of the business associate agree to the same terms and conditions that the business associate has agreed to with respect to the PHI; (e) Ensure that any agents or subcontractors are able to provide each of the individual rights; (f) Make all internal practices , books, records relating to the uses and disclosures of PHI available to the Secretary of the U.S. Department of Health & Human Services; (g) At the end of the business agreement return or destroy all PHI, however, if return or destruction is determined not to be feasible, the protections of the business associate agreement shall continue for as long as the business associate retains the PHI; (h) A term and termination clause, including a termination clause which specifies the effect of termination and any reference to a later survival clause or section.

7. If the business associate violates a material term of the business associate agreement, the business associate agreement shall be terminated. IF termination is not feasible, the problem shall be reported to the Secretary of the U.S. Department of Health & Human Services.
8. Liberty's Business Associate Agreement shall include a requirement that the business associate implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI.
9. Liberty's Business Associate Agreement shall include a requirement that the business associate ensure that any agents or subcontractors agree to implement reasonable and appropriate safeguards to protect electronic PHI.
10. Liberty's Business Associate Agreement shall require that all security incidents are reported to Liberty.
11. Liberty's Business Agreement contains specific clauses with regard to how the business associate shall meet the requirements of Breach Notification Rule (45 C.F.R. 164.400-164.414).
12. Liberty's Business Agreement contains a section requiring the business associate to use Standard Transactions and Code Sets (45 C.F.R. 162.923).
13. If Liberty discovers or suspects that a business associate is inappropriately using or disclosing or failing to protect PHI, Liberty's Privacy Officer shall immediately investigate the concern and notify the Senior Vice President/Chief Operating Officer and General Counsel. If the concern is determined to be valid following a dialogue between Liberty's Privacy Officer, Senior Vice President/Chief Operating Officer and General Counsel, Liberty's Privacy Officer shall notify the appropriate Liberty leadership of the concern and take appropriate follow-up given the level of concern.
14. Liberty shall routinely review business associate relationships and contracts to ensure compliance with the requirement that all business associates maintain a business associate agreement.

II. Client Agreements

1. Prior to entering into any client agreement (whether it be a public or private client), Liberty shall identify and determine whether it is a business associate. If there is a question as to whether a business associate agreement is necessary, both Liberty's Privacy Officer and General Counsel shall be consulted.
2. The Liberty client shall either (a) be provided with Liberty's standard business associate agreement or (b) provide a copy to Liberty of their standard business associate agreement. If a modification is made to Liberty's standard business associate agreement, the documents will be referred to Liberty's Privacy Officer for review and response.
3. All business associate agreements shall have, at a minimum, each of the clauses as required by law and identified above in this SOP.

Regulatory References

45 C.F.R. 164.400-164.414
45 C.F.R. 162.923
45 C.F.R. 160.103
45 C.F.R. 164.308(b)
45 C.F.R. 164.410
45 C.F.R 164.502(e)
45 C.F.R. 164.504(e)
45 C.R.R. 164.530(c)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:56:13 -05'00'

Return to Index

Liberty QualityCare® Liberty Healthcare Corporation HIPAA Standard Operating Procedure #8: Right to Request Restrictions and Confidential Communication

Title:	**HIPAA Right to Request Restrictions and Confidential Communication**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Individuals may request that Liberty's covered entity or business associate clients restrict how the covered entity client, business associate client and Liberty uses or discloses their Protected Health Information (PHI) for treatment, payment, or health care operations. Generally, Liberty shall not be a direct recipient of the request for restrictions or confidential communications. Liberty shall implement restrictions requested by clients or if Liberty is the covered entity, the individual. Liberty shall ensure all requests for restrictions are handled in accordance with the law and as expeditiously as possible.

PROCEDURE

1. All requests for restrictions shall be put into writing and contain enough specific information that Liberty's Privacy Officer shall act with a full understanding of the individual's request. If a request is received orally, the individual requesting such restriction shall be asked to document the request in writing to ensure the request is understood. All such requests shall be forwarded to the appropriate covered entity or business associate client in accordance with applicable business associate agreement provisions. If the covered entity or business associate client agrees to the restriction, in general, the restriction does not prevent the following uses or disclosures: (a) to the Secretary of U.S. Department of Health & Human Services for an investigation to determine compliance with the HIPAA Rules or (b) when the Privacy Rule does not require the covered entity to obtain the individual's authorization or to give the individual an opportunity to object (*i.e.*, those that are required by law, for public health activities, concerning victims of abuse, neglect, or domestic violence, for health oversight activities, for judicial and administrative proceedings, for law enforcement purposes, about decedents, to avert serious threat to health or safety, for specialized government functions or for worker's compensation purposes).
2. The client may terminate a previously agreed upon restriction for several reasons. These reasons include: (a) the individual agrees to or requests the termination or (b) the covered entity informs the individual it is terminating the restriction agreement. The termination is only effective with respect to PHI created or received by the covered entity after it has informed the individual of the termination. Liberty's Privacy Officer, when notified by clients, shall fully document the termination of the restriction including all applicable dates.
3. Liberty shall notify all business associate subcontractors of any restrictions which have been established through Liberty's Privacy Officer. All such notifications shall be memorialized in writing and maintained by the Privacy Officer.
4. Record Retention: All requests and associate response regarding restrictions to PHI shall be documented and retained for a minimum of six (6) years.

Regulatory References

45 C.F.R 164.502
45 C.F.R. 164.522

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:56:37 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #9:
Tracking and Accounting of Disclosures of PHI

Title:	**HIPAA – Tracking and Accounting of Disclosures of Protected Health Information**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall track and document specific disclosures of Protected Health Information (PHI) made by Liberty or its business associates. Individuals have the right to request an accounting of every use or disclosure of PHI relating to the individual—other than for treatment, payment, health care operations, or law enforcement issues to include but not limited to comply with a court order, to respond to a subpoena or to identify or locate a suspect—that have been made by Liberty or its business associate.

PROCEDURE

1. Liberty's Privacy Officer shall respond to any requests for an accounting of disclosures made to Liberty.
2. Liberty, as a business associate of health care providers and health plans, does not expect to receive requests for written accounting of disclosures of PHI directly from individuals. Should Liberty receive such a request as a covered entity, Liberty shall respond as outlined in this Standard Operating Procedure (SOP) and in the business agreement in place with the applicable provider.
3. Liberty shall provide, or cause its business associate subcontractors to provide to its client, an accounting for any individual requesting such accounting. Liberty shall provide the accounting to its client so the client can remit to the individual in compliance with HIPAA mandated timeframes. Liberty shall also, if necessary, ensure that any business associate subcontractors also provide information relevant to the request for an accounting of disclosures.
4. Liberty shall retain logs for both the requests for Accounting of Disclosures and the Disclosure Tracking Log. However, it is not anticipated that there will be many, if any disclosures of PHI which require accounting.
5. An individual has a right to receive an accounting of disclosures of PHI in the six (6) years prior to the date on which the accounting is requested **except for the following disclosures:** (a) to carry out treatment, payment and health care operations (45 C.F.R. 164.506); (b) to individuals of PHI about them (45 C.F.R. 164.502); (c) pursuant to an authorization (45 C.F.R. 164.508); (d) for national security or intelligence purposes (45 C.F.R. 164.512(K)(2); (e) to correctional institutions or law enforcement agencies that have lawful custody of an inmate (45 C.F.R. 164.512(K)(2); (f) as part of a limited data set (45 C.F.R 164.514(e); (g) that occurred prior to the compliance date for Liberty; or (f) incident to a use or disclosure otherwise permitted or required (45 C.F.R. 164.502).
6. The following types of Disclosures shall be tracked for the purposes of accounting: (a) those required by law; (b) public health activities; (c) health oversight activities; (d) judicial and administrative proceedings; (e) Law enforcement purposes; (f) in order to avert a serious threat to health and safety; (g) specialized government functions (*e.g.*, military and veterans activities; protective services for the President and others_; (h) worker's compensation disclosures necessary to comply with laws relating to worker's compensation programs (**not** including disclosures related to payment); (I) Breaches.

7. Liberty shall require that all requests for accounting be made in writing to ensure the clarity of the request made by the individual. Liberty's Privacy Officer shall request additional information following consultation with the Senior Vice President/Chief Operating Officer and General Counsel OR if the request is not specific enough to respond to the request for accounting.
8. In certain limited circumstances, a health oversight agency or law enforcement official may request that the covered entity suspend an individual right to receive an accounting of the disclosures made to that agency or official. In such instance Liberty's Privacy Officer shall be consulted prior to responding to the client, agency or official regarding such request.

Regulatory References

45 C.F.R. 164.506
45 C.F.R. 164.502
45 C.F.R. 164.508
45 C.F.R. 164.512(K)(2)
45 C.F.R. 164.514(e)
45 C.F.R 164.528

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:56:59 -05'00'

Return to Index

Liberty QualityCare® Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #10:
Right to Request Access to Designated Record Set

Title:	**HIPAA Right to Request Access to Designated Record Set**	**Effective Date:**	**10/03/2014**
Author:	**Privacy Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	**01/18/2016**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty's covered entity customers (and Liberty when a covered entity) have established an individual's right to access and obtain a copy of their Protected Health Information (PHI) maintained by Liberty's records if such record is a part of the Designated Record Set. The right to access PHI is applicable only to health information that is subject to the requirements of the HIPAA rules and is contained within Designated Record Sets maintained by Liberty. Individuals shall generally assert their right to access their Designated Record Sets to their covered entity healthcare providers or health plans, rather than to Liberty (unless Liberty is the covered entity). Should Liberty, as a Covered Entity or as a Business Associate, receive an individual's request to access their Designated Record Set: The Designated Record Set is the group of records, which include (a) medical and billing records about individuals maintained by or for a covered health care provider (b) the enrollment, payment claims adjudication, and case or medical management record systems maintained by or for a health plan; or (c) is used in whole or in part, by or for Liberty as a covered entity to make decisions about covered individuals. Items in the designated record set to be produced do not include, among other things (i) psychotherapy notes; (ii) information compiled for use in criminal, civil or administrative proceeding or action; (iii) employment records; (iv) information which is duplicative in nature – e.g., if a document appears more than once or is maintained separately by a business associate, only one copy needs to be provided) maintained by Liberty, in accordance with this policy and the business associate agreement in place with the covered entity.

PROCEDURE

1. Liberty's Privacy Officer shall serve as the point of contact responsible for receiving and processing all formal requests for access to PHI in Designated Record Set. Individuals shall be asked to make all requests for access in writing. Liberty shall respond to all requests for access to a Designated Record Set as expeditiously as possible.
2. Should Liberty receive a right to access or obtain a copy request from a covered entity, Liberty shall comply with the request as directed by this Standard Operating Procedure (SOP) and the business associate agreement in place with the covered entity.
3. Liberty shall forward any individual requests for access to PHI to the covered entity or business associate client within the time frames required under the business associate agreement.
4. Liberty shall provide the covered entity or business associate client with copies of the designated record set in one of the following forms: (a) a form the individual requests, if the information is readily producible in that form; (b) readable hard copy; (c) another form to which Liberty; the individual mutually agree; and PHI in e-form.
5. Corrections Institution Clients: All requests by inmates shall immediately be brought to the attention of the VPO responsible for the client relationship. The VPO shall immediately contact the Privacy Officer and General Counsel to ensure that the requirements of the Privacy Rule and the contract are fully complied with. Correctional institution clients are permitted to deny, in whole or in part, any request for access by an inmate if obtaining such information could jeopardize the health, safety, security, custody or rehabilitation of the individual or of other inmates, the safety of any officer, employee or other person at the correctional institution responsible for the transportation of the individual.

6. Record Retention: All requests and associate response regarding requesting access (JAS01/18/2016) to PHI shall be documented and retained for a minimum of six (6) years.

Regulatory References

45 C.F.R 164.524

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:57:29 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #11: Security Management

Title:	**HIPAA Security Management**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/18/2018**
Location:	**ALL LOCATIONS**	**Last Revision Date:**	**08/20/2016**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall implement reasonable Security Standard Operating Procedures (SOPs) to comply with the Security standards. Liberty may change these Security SOPs at any time, provided the changes are documented and this documentation is retained for six (6) years from the date of its creation or when it was last in effect, whichever is later. Active, current Security SOPs will be on the employee self-service section of Unicorn system with the current most recent review date identified so that the SOPs shall be available to Liberty's workforce members who are responsible for implementation of the SOPs. In addition, Liberty shall maintain a reasonable process to review its SOPs following an evaluation or risk assessment. Notification to Liberty's workforce members of SOPs changes will occur on the employee self service. Liberty's Security Officer shall maintain security management systems in order to identify any risks, vulnerabilities or threats to the confidentiality, integrity and availability of the electronic protected health information (ePHI) and the adoption of reasonable and appropriate measures to reduce any risks, vulnerabilities or threats to the security, confidentiality, integrity and availability of ePHI. Liberty shall, on a regular basis, review and update its Security Management Program SOPs. This Standard Operating Procedure (SOP) applies to all systems which are used to maintain, use, disclose, create, receive or transmit ePHI. Definitions to clarify how risks, vulnerabilities and threats fit together are described at the end of this SOP.

PROCEDURE

Risk Assessment

1. Liberty's Security Officer shall be responsible for the Security Management Process and ensuring that systems that access create or delete events needed to support compliance with HIPAA Security Rule 164.308(a)(iii) – Information System Activity Review-revised ELI 08/20/2015 will be logged and that a mechanism shall exist to make the review practical.
2. Liberty's Security Management Process shall include the assessment of the administrative, physical, and technical aspects for the confidentiality, integrity and availability of ePHI.
3. Liberty's Security Officer shall be responsible for conducting a risk analysis to assess the potential risks and the confidentiality, integrity, and availability of the ePHI. The Risk Analysis is an eight (8) step process including:
    a. Step 1 – ePHI boundary definition (Includes an inventory of information system hardware and software details, including):
        (i) internal and external interfaces,
        (ii) the identification of primary users of the information systems of ePHI,
        (iii) basic function and purpose of the ePHI and information system, and
        (iv) technical controls (*e.g.*, encryption) and non-technical controls (*e.g., SOP*).

b. Step 2 – Threat identification Liberty's Security Officer shall identify and log all potential and actual threats to ePHI. The confidentiality of ePHI shall be determined by analyzing the risk of improper access to stored information, and by the risk of interception, confidentiality, integrity, and availability during electronic transmission of the information.

c. Step 3 – Vulnerability identification Liberty's Security Officer shall identify and log any risk to the confidentiality, integrity and availability of e-PHI, identifying how and why the ePHI has been threatened.

d. Step 4 – Security Control Analysis Liberty's Security Officer shall coordinate with General Counsel in organizing a security control analysis that shall be conducted and logged by a consultant so that a template will be created to use throughout Liberty. This analysis shall include reviews of logs, access reports, and incident tracking. Liberty's Security Officer shall determine whether the controls are adequately preventing threats.

e. Step 5 – Risk likelihood determination Liberty's Security Officer shall make a determination of residual risk of realized risk by reviewing the consultant's security control analysis and comparing it to potential and actual threats and vulnerabilities throughout Liberty and this data shall be logged.

f. Step 6 – Impact Analysis Liberty's Security Officer in coordination with the Liberty consultant shall conduct an impact analysis to determine whether new or modified security safeguards and procedures beyond what Liberty has in place shall be established. This data shall be logged.

g. Step 7 – Risk Determination Liberty's Security Officer shall determine the probability and impact of realized risk, and shall record such information.

h. Step 8 – Security control and recommendations Liberty's Security Officer and when appropriate in conjunction with Liberty's Privacy Officer shall utilize all of the information gathered in the risk analysis and shall develop security control recommendations and shall record such information.

4. In addition to the annual risk analysis, Liberty's Security Officer shall conduct an appropriate risk assessment when an operational or business change would impact the flow of ePHI.

5. Once the risk analysis has been completed, Liberty's Security Officer shall be responsible for the development and updating of SOP to implement any reasonable and appropriate measures to mitigate any risks or e-PHI vulnerabilities to confidentiality, integrity or availability are identified.

6. As part of the Security Management Process, Liberty's Security Officer shall implement SOPs to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports as required by this existing SOP.

7. The Security Officer shall be responsible for the Change Management Process and ensuring that modifications to hardware, software, firmware and documentation do not compromise the security, confidentiality, integrity and availability of Liberty information systems and are implemented in compliance with the HIPAA program and Liberty's obligations regarding ePHI:

   a. All purchase of software or hardware shall be reviewed by Liberty's Security Officer and follow the Change Control Standard Operating Procedure. Liberty's Security Officer shall give approval before new software or hardware is installed or connected to Liberty's networks.

   b. Liberty does not use automatic updates on critical systems and shall instead proceed with such updates using the formal Change Control Standard Operating Procedure.

   c. A formal change request shall be submitted to Liberty's Security Officer AND approved before any change is initiated.

   d. BEFORE approving a change request, Liberty's Security Officer shall conduct a risk analysis to assess the vulnerabilities to confidentiality, integrity, availability, impact, and risks related to ePHI that are associated with the proposed change.

e. To the extent that an emergency change is required to respond to an imminent system failure or to restore service and a change request cannot be submitted prior to the change, a formal change request shall be submitted after execution of the change. Liberty's Security Officer shall immediately perform a risk analysis to determine the impact of the change and any necessary response, and to ensure that the security, confidentially, integrity and availability of the Liberty information systems have not been compromised.

8. The Liberty Security Officer, or designee, shall be responsible for documenting the procedures and reviews. Such documentation shall be maintained by the Liberty Security Officer.

For the purposes of this SOP:

the following definitions adapted from NIST SP 800-30 shall be used to clarify how risks, vulnerabilities and threats fit together:

Risk:

The net mission impact considering (1) the probability that a particular threat will exercise (accidentally or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur. Risks arise from legal liability or mission loss due to:

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
- Unintentional errors or omissions
- IT disruptions due to natural or man-made disasters
- Failure to exercise due care and diligence in the implementation and operation of the IT systems

Vulnerability:

A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of Liberty's security SOPs.

Threat:

The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability:

- Natural threats such as floods, earthquakes, tornadoes, and landslides
- Human threats are enabled or caused by humans and may include intentional (e.g. Network and computer based attacks, malicious software upload, and unauthorized access to e-PHI) or unintentional (e.g. inadvertent data entry or deletion and inaccurate data entry) actions

Environmental threats such as power failures, pollution, chemicals, and liquid leakage.

Regulatory References

45 C.F.R. 164.308
45 C.F.R 164.308(a)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:57:58 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #12:
Right to Request an Amendment to PHI

Title:	**HIPAA Right to Request an Amendment to Protected Health Information**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/18/2018**
Location:	**ALL LOCATIONS**	**Last Revision Date:**	**01/18/2016**
Functional Area:	**ADMINISTRATION**		

POLICY

Individuals shall have the right to request an amendment to their PHI in a Designated Record Set, including PHI maintained by Liberty on behalf of its covered entity or business associate clients. A Designated Record Set means: (1) A group of records maintained by or for a covered entity that is: (a) The medical records and billing records about individuals maintained by or for a covered health care provider; (b) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (c) used, in whole or in part, by or for the covered entity to make decisions about individuals (45 C.F.R. 164.501). The term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity (45 C.F.R. 164.501). Individuals will generally request an amendment from the covered entity or business associate client, rather than to Liberty. Should an individual contact Liberty directly, Liberty shall respond as outlined in this Standard Operating Procedure and in the business associate agreement in place with the applicable client. Liberty shall review and implement all requests for amendment in compliance with the law and as expeditiously as possible.

PROCEDURE

1. Liberty's Privacy Officer shall serve as the point of contact responsible for receiving and processing all formal requests for amendment to PHI. Covered entity clients and individuals will be asked to make all requests for amendment in writing.
2. Requests for Amendments from Covered Entities: If Liberty in its capacity as a business associate, receives a request for amendment to PHI from a covered entity, such request shall be forwarded to Liberty's Privacy Officer. Liberty's Privacy Officer shall evaluate the request to determine whether Liberty maintains the PHI in a Designated Record Set. Liberty shall comply with the covered entity's request to the extent that Liberty maintains the PHI at issue in a Designated Record Set. In processing any request for amendment from a covered entity, Liberty shall follow the requirements set for in 45 C.F.R. 164.526 and applicable business associate agreement.
3. Requests for Amendments from Individuals: In rare instances, individuals may make a request for amendment to the PHI that Liberty shall maintain in a Designated Record Set directly to Liberty. An amendment may include corrections, changes or clarifications requested by the individual. Any request for amendment must be in writing and shall be directed to Liberty's Privacy Officer. Liberty's Privacy Officer shall consult the applicable business associate agreement AND notify the applicable covered entity client. All amendment requests shall be processed within the time frames specified by HIPAA.
4. Record Retention: All requests and associate response regarding amendments (JAS01/18/2016) to PHI shall be documented and retained for a minimum of six (6) years.

Regulatory References

45 C.F.R. 164.501
45 C.F.R. 164.526

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:58:24 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #13: Security Officer

Title:	**HIPAA Security Officer**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/18/2018**
Location:	**ALL LOCATIONS**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall have a Security Officer to oversee and implement the Security Program and to work to ensure Liberty's compliance with the requirements of the HIPAA Security Standards. Liberty's Security Officer shall be responsible for handling all security issues related to electronic Personal Health Information (e-PHI) and is responsible for the development and implementation of the Standard Operating Procedures (SOPs) required by HIPAA's Security Rule.

PROCEDURE

1. Liberty's Security Officer or designee shall be responsible for documenting the SOPs and reviews to discern whether HIPAA compliance is current. Such documentation shall be maintained by Liberty's Security Officer.
2. Liberty's Security Officer shall provide oversight for (a) Security Standard Operating Procedures (SOPs) and (b) developing, communicating and implementing Liberty's Information Security Program.
3. Liberty's Security Officer shall support training for all Liberty workforce members related to Information Security. While training is overseen by Liberty's Privacy Officer, Liberty's Security Officer shall provide support on all security related issues. Liberty's Security Officer shall periodically send security reminders on Liberty's intranet or via e-mail.
4. Liberty's Security Officer shall work in conjunction with Human Resources to ensure that violations of the Security management and any associated SOPs shall be addressed. Liberty's Security Officer shall document any sanctions that are applied and such documentation shall be maintained by Human Resources.
5. Liberty's Security Officer shall mitigate, to the extent practicable, any security issue that is known to Liberty.
6. Liberty's Security Officer, when appropriate, works with Liberty's Privacy Officer should there be any data security incidents for investigation and to report any breach of PHI or personal information that may require notification to individuals and any regulators.
7. Liberty's Security Officer shall revise any SOPs related to Security with any changes in operations or changes in the law.
8. Liberty's Security Officer shall ensure appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity and availability of ePHI from an intentional or unintentional use or disclosure that is in violation of the Security SOPs.
9. Liberty's Security Officer shall conduct periodic risk analysis of the systems as required by the Security Management SOP.
10. Liberty's Security Officer, in conjunction with the Privacy Officer, shall ensure business associate subcontractors agree to implement reasonable and appropriate security measures and execute a business associate agreement.

Regulatory References

45 C.F.R. 164.308(a)(2)

45 C.F.R 164.308(a)(5)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:58:50 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #14: Information Access Management

Title:	**HIPAA Information Access Management**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall have a Security Officer to oversee and implement the Security Program and to work to ensure Liberty's compliance with the requirements of the HIPAA Security Standards. Liberty's Security Officer shall be responsible for handling all security issues related to electronic Personal Health Information (e-PHI).

PROCEDURE

Access Authorization

a. The Security Officer in consultation with the Privacy Officer shall define and authorize all access to information systems containing or accessing ePHI.

b. Access to ePHI is only granted to workforce members who require specific information to accomplish the work responsibilities of their position, and is granted on a minimum necessary or need-to-know basis. Liberty workforce members are not allowed to access information systems containing or accessing ePHI until properly authorized. Access is specified, documented, reviewed periodically, and revised as necessary.

c. Liberty workforce members shall not attempt to gain access to information systems which contain or access ePHI for which they have not been given proper authorization or access.

d. Access authorization for new members of Liberty workforce shall be performed in compliance with the "Workforce Security" SOP.

e. All members of the workforce with access to Liberty information systems shall be assigned a unique user ID.

Access Establishment and Modification

a. Liberty shall have a documented process for authorizing, documenting, reviewing and modifying access to information systems containing ePHI which is maintained and implemented by Liberty's Security Officer and with Human Resources.

b. The Security Officer, in conjunction with the Privacy Officer, shall define and authorize all access to information systems containing ePHI. Access to secure shared drive storage, secured personal network drive storage, and any other area (or software) that contains ePHI access is discretionary to the Security Officer and Privacy Officer.

c. The Security Officer shall periodically review User access rights to information systems containing ePHI to ensure that they are provided only to those who have a need for specific ePHI in order to accomplish a legitimate task.

d. All revisions to Liberty's workforce member's access rights shall be tracked, logged and audited. The Security Officer shall obtain a list of log-in information from the Liberty programs to the secured shared drive on a quarterly basis.

e. Access to information systems containing ePHI shall be authorized only for users having a need for specific information in order to accomplish a legitimate task. All such access shall be defined and documented. Such access shall also be periodically reviewed and revised as necessary.

f. When accessing ePHI through a remote connection, Liberty's workforce members shall do what is reasonable through use of a secure connection. ePHI accessed through a public wireless or Wi-Fi connection shall be with a secure connection only. All remote access shall be made in conformance with the Remote Access SOP.

Regulatory References

45 C.F.R. 164.308(a)(4)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:59:13 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #15: Workforce Security

Title:	**HIPAA Workforce Security**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	**12/14/2015**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall be committed to limiting access to Electronic Protected Health Information (ePHI) only to appropriate Liberty workforce members and to preventing those Liberty workforce members who do not need access to ePHI from obtaining such access. Liberty shall maintain appropriate Standard Operating Procedures (SOPs) to ensure that all Liberty workforce members have appropriate access to ePHI.

PROCEDURE

1. Liberty's Privacy Officer shall ensure that all Liberty Workforce members who access ePHI have the necessary knowledge, skills, and abilities to fulfill positions involving access to and use of sensitive information as confirmed by pre-hire competency evaluations completed by Liberty's Privacy Officer. Liberty's Security Officer shall designate all Liberty's workforce members to the level of ePHI access they will have.
2. Each Liberty workforce member with access to ePHI shall have a direct supervisor who is aware of the access to ePHI and IF the supervisor is changed or the Liberty workforce member has a change in title or responsibility, such access shall be re-examined.
3. Any Liberty workforce member who is removed from having access to ePHI for any reason, including disability, change of work assignment, vacation or termination for any reason, shall immediately return his or her Liberty workforce member identification to the Vice President of Human Resources or the Hiring Manager: (a) The Vice President of Human Resources or the Hiring Manager shall recover all access control devices (i.e. ID badges, keys, access cards) when Liberty employment or the physician subcontractor contract ends; (b) Liberty's Security Officer shall deactivate computer access accounts in accordance with the SOP for Liberty's workforce members termination.
4. The Vice President of Human Resources shall document any security breaches that have resulted in terminations.

Regulatory References

45 C.F.R. 164.308(a)(3)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 13:59:38 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #16:
Security Awareness and Training

Title:	**HIPAA – Security Awareness and Training**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	**12/14/2015**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall implement a security awareness and training program for all of Liberty's workforce members to ensure an understanding of the roles and responsibilities of Liberty's workforce members with access to electronic Personal Health Information (ePHI) to maintain the security, confidentiality, availability and integrity of the ePHI.

PROCEDURE

1. Liberty's Security Officer shall routinely remind Liberty's workforce members of security issues and protocols and security updates.
2. Liberty shall routinely remind Liberty's workforce members about procedures for guarding against, detecting and reporting malicious software: *See* "Protection from Malicious Software" Standard Operating Procedure (SOP).
3. Liberty shall monitor log-in attempts and routinely report to the Liberty workforce members information about log-in attempts and discrepancies:
    a. At a minimum, the events shall be tracked where ePHI is maintained and reviewed on a weekly basis for trends or other indications that unauthorized access or other security events are maintained.
    b. All logs are backed up and retained off-site for a minimum of (6) years:
        i. User ID,
        ii. Dates and times of logon and logoff,
        iii. Logon method, location, terminal identity, Network address,
        iv. Record of unsuccessful system access attempts,
        v. Records of successful and rejected data access and other resource access attempts,
        vi. Access to powerful system utilities,
        vii. Access to ePHI files or directories;
        viii. Other security operational documents (e.g. facility entry logs, audits, assessments, breach analysis/notification and evaluations).
    c. Liberty' Security Officer shall review audit logs on a daily basis using the concept of exception only. Additional key events and criteria are established as needed by Liberty in order to determine what events are relevant to the environment and require review and follow-up action. Security Events Monitoring (SEM) applications OR similar database applications are used to define event criteria and attempt to correlate suspicious events and provide the data necessary to investigate the situation. All irregular events are reported to Liberty's Security Officer and Liberty expects that the Standard Operating Procedure (SOP) "Data Incident" shall be followed; (c) Liberty's Security Officer shall review security events and other logs on a weekly basis utilizing a database management solution (i.e. NetIQ). Potential security exposures are reviewed, investigated and corrective action taken when necessary.

4. Within any specific computing environment, Liberty's workforce members will review the Security SOPs (via employee self-service) for the creating, changing and safeguarding of passwords. In any application or processing platform, the ability of general users to access files, containing passwords shall be limited:

    a. Access of password files by Users shall be monitored for unauthorized activity where possible. When possible, the password file shall be encrypted to make the passwords unreadable to anyone who possesses the file;

    b. At a minimum, the following items shall be implemented within Liberty applications and processing platforms:

        i. All users shall require a unique user ID and shall not be allowed to share user accounts and respective passwords.
        ii. All Liberty passwords shall have a minimum of 8 characters in length,
        iii. Passwords for high-risk ePHI shall automatically expire every 90 days. Passwords for low and medium-risk ePHI shall expire every 180 days. E.B 12/14/15
        iv. Passwords used to access ePHI shall contain both upper and lower case characters (i.e. a-z, A-Z) and at least one numeric or special character,
        v. When new systems or applications are brought on-line, all default (first use) passwords shall be changed immediately upon use,
        vi. End-users shall be allowed 3 grace logins to change their password once the existing password has expired,
        vii. Null passwords, or passwords which are the same as user ID's shall not be allowed,
        viii. The user's past four or more passwords shall be remembered and not available for use within the given application.
        ix. Dates and times of logon and logoff,
        x. For terminations with ePHI, timeouts shall be invoked after 15 minutes of inactivity and shall be password protected,
        xi. All system – level passwords (i.e. root, enable NT admin, application, administrative accounts, etc.) shall be changed on an annual basis or as needed when a Liberty workforce member with administrative privileges leave or no longer require access;

Regulatory References

45 C.F.R. 164.308(a)(5)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:00:03 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #17: Contingency and Disaster Recovery Plan

Title:	**HIPAA – Contingency and Disaster Recovery Plan**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	**08/20/2015**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall maintain a Standard Operating Procedure (SOP) for Emergency/ Business Interruption Disaster Plan that includes the steps to take in responding to an emergency or other occurrence (for example fire, vandalism, system failure and natural disaster) that damages systems and/or applications containing ePHI. While most emergency operations are handled by Business Associates of Liberty, Liberty takes several steps to ensure the confidentiality, availability and integrity of ePHI especially when Liberty is the covered entity.

PROCEDURE

1. Liberty's Security Officer shall maintain a Data Back UP system: (a) Liberty shall send tape copies of all servers, including ePHI to an off-site facility. In the event of an emergency, and only as necessary, the latest tapes shall be recovered back for server restoration and Liberty shall cross check the restored ePHI to ensure accuracy; (b) All media transferred to off-site locations shall be placed in secure containers identified by media labels indicating the contents are Liberty's. Liberty authorized personnel or the off-site storage vendor shall be the only individuals authorized to transport media to and from the off-site location; (c) All backup media stored off-site shall be inventoried by both Liberty and the off-site storage of the Business Associate.
2. Liberty's Security Officer shall maintain information for a Disaster Recovery Plan for ePHI: (a) Liberty shall restore lost, damaged or destroyed ePHI from regularly maintained backups, or outside sources (i.e. vendors). The electronic re-installation of ePHI due to disaster shall be reviewed based on Liberty's Standard Operating Procedure (SOP) "Electronic Media Backup"; (b) Liberty's Security Officer shall maintain Liberty's Emergency/Business Interruption Disaster Plan that shall outline Liberty's operations and needs. Liberty's Emergency/Business Interruption Disaster Plan shall be maintained on Liberty's Intranet.
3. Liberty's Security Officer shall maintain information on Emergency Mode Operations to Liberty's Emergency/ Business Interruption Disaster Plan SOP that outlines what Liberty will do during an emergency until Liberty-owned servers are restored. Once electronic data is restored to protected servers at Liberty, business shall be conducted as usual.
4. Liberty's Security Officer shall maintain testing and revising contingency plans: (a) All tests and revisions shall be determined on an "as needed basis", and Liberty shall update any improvements towards security, expediency, and cost effectiveness: (b) Contingency backups, recovery plans, loss and destruction of data and many other components of data restoration shall be scrutinized for effectiveness and possible improvement; (c) Other logistics may include budgetary concerns and time availability of personnel (the latter logistics apply ONLY on the addressable items). (d) Actual test of the recovery plans shall be conducted periodically and revisions to recovery plans made according to the outcome of tests. revised ELI08/20/2015
5. Liberty's Security Officer shall assess the relative criticality of specific applications and data support of other contingency plan components as an application and data criticality analysis

6. At a minimum, Liberty shall perform an annual risk assessment of ePHI: Contingency backups, recovery plans, loss and destruction of data and many other components of data restoration are scrutinized for effectiveness and possible improvement.

Regulatory References

45 C.F.R. 164.308(a)(7)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:00:33 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #18: Asset Tracking

Title:	**HIPAA – Asset Tracking**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall track assets by their location and by who is using them which shall help prevent the loss of data by tracking Liberty assets. This Information is critical to have on hand in the event a device containing ePHI is breached, lost or stolen.

PROCEDURE

1. Liberty's Security Officer shall track the following assets (owned or leased): (a) Desktop workstations; (b) Laptop computers; (c) Scanners, copy machines and fax machines; and (d) Handheld devices, including Blackberries, iPhones, IPads, Palm pilots and other smart phones. USB/Thumb drives and other similar portable devices shall be tracked despite their minimal use.
2. Liberty's Security Officer shall maintain a tracking database that tracks the following information for each Liberty device listed above: (a) Serial number; (b) Asset type and brand; (c) Current location; (d) Designated Liberty workforce member; (e) Access to ePHI; (f) Password protection installation; (g) When the device has been encrypted and to what level encryption standard has been met.
3. When Liberty acquires a new asset, the asset shall be labeled as property of Liberty and Liberty's Security Officer or designee shall immediately add the asset to the asset database before assigning the asset to a Liberty workforce member. Devices, with the exception of scanners, copiers and fax machines, shall not be distributed to Liberty's workforce members until they are password protected.
4. Whenever a tracked asset is transferred to a different Liberty workforce member or moved to a new location, Liberty's Security Officer shall be notified and shall update the information in the asset database as soon as possible. If an asset is disposed of, the asset shall remain in the asset database with a location of "destroyed". Any reuse or disposal of any asset shall be conducted in accord with Liberty's Standard Operating Procedure (SOP), "Device and Media Controls".
5. All Liberty workforce members shall be required to notify both the Vice President of Human Resources and Liberty's Security Officer immediately upon discovering that an asset has been lost or stolen. Whenever a Liberty asset is lost or stolen, the designated Liberty workforce member shall follow Liberty's "Portable Computing Device" SOP. Liberty's Security Officer shall update the asset's location in the asset database as "Lost or Stolen". Refer to Liberty's SOP "Security Incident".

Regulatory References

45 C.F.R. 164.310(d)(1)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:00:58 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #19:
Data Integrity for ePHI

Title:	**HIPAA Data Integrity for ePHI**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/18/2018**
Location:	**All Locations**	**Last Revision Date:**	**12/14/2015**
Functional Area:	**ADMINISTRATION**		

POLICY

There can be a number of security incidents related to use of laptops, other portable and/or mobile devices and external hardware that store, contain or are used to access Electronic Protected Health Information (EPHI) under the responsibility of Liberty and our customers who are a HIPAA covered entity. This is particularly relevant for Liberty programs that allow remote access to EPHI through portable devices or on external systems or hardware not owned or managed by Liberty. The main objective of this Liberty policy is to reinforce some of the ways Liberty shall protect EPHI when it is accessed or used outside of Liberty's physical purview. The procedure below will set forth strategies that shall be reasonable and appropriate for Liberty programs that conduct some of their business activities through the use of portable media/devices (such as USB flash drives and Memory cards, floppy dicks, CDs, DVDs) that store EPHI and/or have access or transport EPHI via tablets, laptops, Smart Phones, backup media, email, hotel, library, (or other public workstations) , Wireless Access Points (WAPs); personal digital assistants (PDAs), home computers, Remote Access Devices (including security hardware) or other non-corporate equipment. Liberty shall be extremely cautious about allowing the offsite use of or access to EPHI and this Standard Operating Procedure (SOP) and Liberty's workforce member's training shall be effectively deployed to all of Liberty programs so that Liberty consistently complies with the applicable requirements of the HIPAA Privacy Rule.

PROCEDURE

Data Integrity for EPHI

1. **Log-on password information:**
   a. ~~Liberty shall implement two-factor authentication for granting remote access to systems that contain EPHI. This process shall require factors beyond general usernames and passwords to gain access to systems (e.g. requiring users to answer a security question such as "favorite pet's name").~~E.B 12/14/2015
   b. Liberty shall implement a technical process for creating unique user names and performing authentication when granting remote access to Liberty's workforce members. (Liberty may use a Remote Authentication Dial-In User Service [RADIUS] or other similar tools).
2. **Employee access to EPHI**
   a. Prior to granting remote access, each Liberty workforce member shall be assigned their level of remote access.
   b. Prior to granting remote access, each Liberty workforce member shall have training on this remote access and this training shall be verified and documented.
3. **Home or other offsite workstations:**
   a. Liberty shall establish time-out session defaults for termination on inactive portable or remote devices.

4. **Contamination of systems:**

   a. Liberty shall install personal firewall software on all tablets, laptops that store or access EPHI or connect to networks on which EPHI is accessible.

   b. Liberty shall install, use and regularly update virus-protection software on all portable or remote devices that access EPHI.

5. **Storing EPHI**

   a. An inventory control system shall be developed to track all types of hardware and electronic media such as hard drives, magnetic tapes or disks, optical disks or digital memory cards, and security equipment.

   b. A process shall be implemented that maintains a record of the movements of and person (s) responsible for, or permitted to use hardware and electronic media containing EPHI.

   c. Unattended tablets and laptops shall have a lock-down mechanism.

   d. There shall be encryption and password protection for files on Smart Phones, tablets or laptops.

   e. There shall be encryption with appropriate strength and password protection on all portable and remote devises that store EPHI.

   f. Appropriate Security updates shall be deployed to portable devices such as Smart Phones, tablets, PDAs and laptops on a regular basis.

   g. Liberty shall consider the use of biometrics, such as fingerprint readers on portable devices based on cost/benefit.

   h. All EPHI entered into the remote systems shall have a backup process.

   i. Encryption protection shall be on the backup and archival media and shall be of appropriate strength.

   j. There shall be a complete deletion of all disks and backup media prior to disposal which may include physical destruction.

   k. The downloading of EPHI onto remote systems or devices shall be prohibited without an operational justification.

   l. Liberty workforce members shall be trained on this SOP in its entirety including how to delete any files intentionally or unintentionally saved to an external drive.

   m. Minimize the use of browser-cached data in web based applications which manage EPHI, particularly those accessed remotely.

   n. Virus-protection software shall be installed on all portable or remote devices that store EPHI.

6. **Transmitting EPHI:**

   a. Transmission of EPHI via open networks, such as the Internet shall be permitted only with a secure connection.

   b. The use of offsite devices or wireless access points (e.g. hotel workstations) is permitted for non-secure access to email and when such access points are with a secure connection.

   c. Liberty shall use a secure connection for email via SSL and the use of message-level standards such as S/MIME, SER, PEM, PGP, etc.

   d. Liberty shall implement and mandate appropriately strong encryption solutions for transmission of EPHI (e.g. SSL (minimum requirement), HTTPS, etc.).

   e. Virus – Protection software shall be installed on portable devices that can be used to transmit EPHI.

Regulatory References

45 C.F.R. 164.310
45 C.F.R. 164.312

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:05:48 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #20: Data/Security Incidents

Title:	**HIPAA - Data/Security Incidents**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	**12/20/2018**
Functional Area:	**ADMINISTRATION**		

POLICY

This Standard Operating Procedure (SOP) applies to Data Incidents. Data incidents include all suspected and actual impermissible uses and disclosures, Security Incidents, breaches of Unsecured Protected Health Information (PHI) and breaches of "personal information" as defined by state law. This SOP shall also be used when a Liberty workforce member suspects and reports a Data Incident and incidents involving data integrity and data availability.- revised 08/20/2015

PROCEDURE

1. All Liberty workforce members shall be responsible to report any information regarding Data Incidents as quickly as possible to their supervisor/direct report. This supervisor/direct report shall immediately contact at a minimum Liberty's Privacy Office and the Vice President of Operations (VPO). Liberty's Privacy Officer shall notify Liberty's Senior Vice President/Chief Operations Officer and General Counsel of the Data Incident. (12/20/2018)
2. If Liberty is the business associate, the VPO 12/20/2018 shall notify the covered entity of the discovery of a breach of unsecured protected health information. A breach shall be considered discovered by a business associate, as of the first day on which the breach is known. To the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during a breach.
    a. Liberty's Privacy Office and VPO shall respond and quickly analyze the Data Incident to determine the level of risk and potential harm and to determine the level of response. (12/20/2018) In collaboration with the Senior Vice President and General Counsel 12/20/2018, this team shall assign one of the four category levels, which will dictate the response expectations:

        Level 1- A threat to sensitive data (such as PHI)
        Level 2- A threat to computer systems
        Level 3- A disruption of services
        Level 4- No threat

    b. Liberty's Privacy Office and VPO (12/20/2018) shall mitigate, if possible, any harmful effects of the Data Incident.
    c. Liberty's Privacy Officer shall document the Data /Security incident and its resolution.
    d. Liberty shall provide notification of any breaches of PHI and of Personal Information as required by law.

Examples of Data / Security Incidents:

- Loss of service, equipment or facilities,
- System malfunctions or overloads, human errors,
- Non-compliance with standard operating procedures,
- Malfunctions of software or hardware,

- Access violations,
- Breaches of confidentiality,
- Integrity of information,
- Any attempted or successful unauthorized access to Liberty's computer network or information systems, specifically excepting "pings",
- Any attempted or successful interference with the normal operations of Liberty's computer network or information systems,
- The unauthorized access, interception, alteration, use, disclosure, or deletion of ePHI, whether secured or insecure.

Regulatory References

45 C.F.R. 164.308(a)(6)
45 C.F.R. 164.400-164.414
16 C.F.R. 318, *et seq.*
74 Fed. Reg. 19006, 19008-10 (April 27,2009)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:01:41 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #21: Security Evaluation

Title:	**HIPAA – Security Evaluation**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	**08/20/2015**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall have ongoing evaluations to identify any new potential risks or vulnerabilities to the confidentiality, integrity or availability of e-PHI as operations and systems evolve. Liberty shall periodically evaluate compliance with the Standard Operating Procedures (SOPs) and practices with the requirement of the HIPAA Security Rule. – revised ELI08/20/2015

PROCEDURE

1. Liberty's Security Officer shall conduct an Information System Evaluations in response to environmental and operational changes. Liberty's Security Officer shall determine if the evaluation should be conducted by internal staff or whether an outside consultant should be engaged.
2. The Security Evaluation shall identify all information systems with access or that maintain ePHI. Each Security Evaluation shall also identify those information systems and associated data that are critical to Liberty's continuing business operations.
3. Any revisions to the Security Evaluation Standard Operating Procedure (SOP) shall be administered through the Security Officer.
4. All elements of the Security Rule shall be considered when conducting the Security Evaluation. Liberty's Security Management Tool may be utilized to document portions of the Security Evaluation, when appropriate.
5. All Security Evaluation findings, remediation options and remediation decisions shall be maintained by Liberty's Security Officer.

Regulatory References

45 C.F.R. 164.308(a)(8)

National Institute of Standards and Technology Special Publication, *Risk Management Guide for Information Technology Systems,* pages 800-830.

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:06:25 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #22:
Facility Access Control

Title:	**HIPAA – Facility Access Control**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	**01/18/2016**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall implement this Standard Operating Procedure (SOP) to limit physical access to its electronic information systems and shall maintain access controls to prevent unauthorized physical access, tampering, and theft to the systems and to the facilities in which they are located, while ensuring that properly authorized access is allowed. These facility access controls are established to protect the security, confidentiality, integrity and availability of its information systems and PHI (JAS01/18/2016).

PROCEDURE

Contingency Operations:

1. Liberty's Security Officer shall establish and implement, if needed, procedures that allow facility access in support of restoration of lost data under Liberty's SOP "Disaster Recovery and Business Interruption Plan" in the event of an emergency.
2. The perimeter of the building or site containing Liberty information systems with ePHI/PHI (JAS01/18/2016) shall be physically sound; the external walls of the site shall be solidly constructed and all external doors have appropriate protections against unauthorized access.
3. Physical barriers, if necessary, shall be extended from actual floor to actual ceiling to prevent unauthorized entry. Doors and windows shall be locked when unattended. Facilities shall be accessible after hours by individually issued keycard access only.
4. All physical access rights to Liberty areas where information systems containing ePHI/PHI (JAS01/18/2016) are maintained shall be regularly reviewed and revised as necessary.
5. Liberty's Security Officer shall implement appropriate safeguards for all equipment containing ePHI. Such equipment includes, but is not limited to: workstations, servers, removable devices, PDAs, laptops.

Facility Security Plan:

6. Liberty shall safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft.
7. Liberty facility delivery and loading areas shall be controlled to prevent unauthorized access.
8. Liberty ensures that, in an event of an emergency or disaster, only authorized Liberty users shall administer or modify processes and controls which protect ePHI contained on information systems.
9. Liberty shall maintain a written facility security plan as a responsibility of the security officer.(JAS08/20/2015)

Access Control and Validation Procedures:

10. Liberty's Security Officer shall control and validate a person's access to facilities based on their role or function, including visitor control of access to software programs for testing or revision.

11. Liberty information systems containing ePHI shall be physically located in areas where unauthorized access is minimized (e.g. servers in locked, climate controlled rooms).

12. Liberty shall perform an annual inventory of all physical assess controls used to protect information systems at its facilities. The inventory report shall be stored in a secure manner and shall be maintained at each facility with a copy to the Liberty's Security Officer.

13. All visitors must show proper identification and sign in prior to gaining physical access to Liberty areas where information systems containing ePHI are located.

Maintenance Records:

14. Liberty's Security Officer shall document repairs and modifications to the physical components of a facility which are related to security (e.g. hardware, walls, doors, and locks).

15. The level of protection provided for Liberty information systems containing ePHI shall be commensurate with that of identified risks. An assessment of risks to Liberty facilities and information systems containing ePHI/PHI (JAS01/18/2016) shall be conducted at least annually in conjunction with the Security Evaluation.

Regulatory References

45 C.F.R. 164.310 (a) – JAS revised 08/20/2015

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:06:51 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #23:
Workstation Use & Security

Title:	**HIPAA - Workstation Use & Security**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall specify the proper functions to be performed at workstations to include the manner in which those functions shall be performed, and the physical attributes of the surroundings of specific workstations or class of workstation that can access electronic protected health information. There shall be restricted access to information systems containing electronic protected health information to properly authorized users only.

PROCEDURE

1. Liberty workstations shall be used only for authorized purposes: to support the business functions of Liberty.
2. Liberty workstations containing ePHI shall be located in physically secure areas and their display screens are positioned so as to prevent unauthorized viewing of ePHI.
3. Users shall not use Liberty workstations to engage in any activity that is either illegal under local, state, federal or international law or is in violation of Liberty's HIPAA Privacy and Security Program SOPs.
4. Users shall adhere to Liberty's Internet and E-Mail Standard Operating Procedures (SOPs).
5. Access to all Liberty workstations containing ePHI shall be controlled by reasonable and appropriate authentication methods. Unique user Ids and passwords shall be used and activity for unique users Ids and passwords shall be tracked.
6. When Liberty workforce members leave Liberty, their information system privileges, both internal and remote, shall be disabled or removed by the time of the departure. Special attention shall be paid to situations where a privilege access user terminates.
7. The display screens of Liberty workstations containing ePHI shall be positioned such that information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception, public or other related areas.
8. Liberty users shall activate workstation locking software whenever they leave their workstation unattended. An automatic lock of the workstation shall happen after a predetermined amount of inactivity. Liberty users shall log off from or lock their workstation(s) before they leave at the end of the day/shift.

Regulatory Reference:

Removed 45 C.F. R. 164.308 (a) (5) – 08/20/2015
45 C.F.R. 164.310(b)& (c)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:07:17 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #24:
Device and Media Controls

Title:	**HIPAA – Device and Media Controls**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall ensure that computer equipment and electronic storage media that contain Electronic Protected Health Information (ePHI) shall be monitored and ePHI shall be disposed of in a secure manner so as to avoid any inadvertent disclosure of any ePHI. Controls shall be maintained for all hardware and software moving into, out of and within Liberty facilities and include both portable and non-portable devices. Electronic storage media includes but is not limited to magnetic tapes, floppy disks, CDs, DVDs, hard disk drives, laptops, copy machines, smart phones, USB/thumb drives or other similar devices used to electronically store data as defined in 45 C.F.R. 160.103.

PROCEDURE

I. Disposal:

1. Liberty's Security Officer shall create a process for the final disposition of ePHI and/or the hardware or electronic media on which it is stored. All Liberty workstations, laptops, and Intel-based servers shall be sanitized using a triple-pass overwrite procedure. Whenever possible the overwrite procedure shall be modeled after the U.S. Department of Defense 5220.22-M Standards (See below for brief summary):
    a. All of Liberty's electronic storage media that is not reused shall be destroyed after its use. The destruction shall be done in accordance with instructions outlined by Liberty's Security Officer and coordinated with vendors to ensure that no ePHI shall be compromised. Such vendor shall be a Business Associate.
    b. Any device or drive that fails to wipe clean shall be fully destroyed. A verification "proof of sanitization" certification for each serial number shall be available to Liberty;
    c. Equipment recognized as having value may be sold. In those cases, hard drives shall be sanitized using a triple-pass overwrite procedure modeled after the U.S. Department of Defense 5220.22-M Standards or destroyed (physical or by degaussing) prior to their sale – All destroyed media e-PHI shall be logged into a database by Liberty's Security Officer:
    d. All back-up tapes shall be maintained by vendors and destroyed in accordance with Liberty's Standard Operating Procedure (SOP). Vendors engaged for the purposes of destruction of backup tapes shall be Business Associates and required by contract to ensure destruction in accordance with HIPAA compliant methodologies;
    e. Prior to returning any leased equipment, including copier machines, fax machines or scanners, the hard drives shall be sanitized and downloaded for retention: (i) Liberty's Security Officer shall ensure that vendors who provide leasing services and management for Liberty shall maintain a record of each piece of equipment on lease by make, model, and serial number

throughout the life of the lease. At the expiration of the lease period, equipment not purchased off lease shall be returned to the leasing company. Liberty shall maintain the following data protection and sanitization process for any Liberty equipment returned to the Corporate Office.

Step 1: Upon arrival at Liberty, returned equipment shall be moved directly into the Security Officer's locked work area with limited access to others.

Step 2: Within this locked work area, all hard drives on all PCs, notebooks and Intel-based servers shall be sanitized using a triple-pass overwrite process modeled after the U.S. Department of Defense 5220.22-M Standards (see below). Any drives that fail to wipe clean shall be fully destroyed.

Step 3: A verification of 'proof of sanitization' shall be maintained by Liberty's Security Officer.

II. Media Reuse:

2. Liberty's Security Officer shall maintain a process for removal of ePHI from electronic media before the media are made available for re-use. Prior to making the determination whether to reuse or dispose of the electronic storage media, all ePHI shall be identified. In limited situations, electronic storage media shall be reused. However, all reuse shall be properly documented and free from any ePHI prior to reuse.

   Equipment recognized as having nominal or no value shall be salvaged. Only approved salvage vendors shall be used. Vendors shall have the capability to meet the U.S. Department of Defense 5220.22 M Standards for data sanitization. Liberty shall require certificates of sanitization, or physical destruction of any hard drives that are sent for salvage. Typically, Liberty shall physically remove and destroy PC/Laptop hard drives before salvaging the PC or Laptop. Liberty shall not salvage Servers or their drives.

   (i) All transactions that include return to lesser, salvage, or sell shall be forwarded to Liberty's Security Officer;
   (ii) Liberty's Security Officer shall create a record with the aforementioned information;
   (iii) Liberty's Security Officer shall provide monthly and year-to-date reporting of all these records to the Liberty's Chief Financial Officer.

III. Accountability:

3. Liberty' Security Officer or designee shall maintain an asset tracking system to record the movements of all hardware and electronic media owned and/or leased by Liberty and any person responsible therefore. This tracking system shall assist Liberty's Security Officer in making sure that no ePHI is inadvertently released or shared with an unauthorized person(s).

IV. data Back-Up and Storage:

4. In general, USB/Thumb drives shall be prohibited to be used and shall not contain any ePHI. Liberty's Security Officer shall make determinations based on the facility and program.

5. Liberty shall maintain data backup files. Liberty's Security Officer shall create a retrievable, exact copy of Electronic Protected Health Information (ePHI), when needed and before movement of equipment. All such back up data shall be retained in accordance with Liberty's Standard Operating Procedure (SOP) for "Document Retention and Maintenance":

   a. All backup tapes shall be maintained by vendors and destroyed in accordance with Liberty SOPs. Vendors engaged for the purposes of destruction of backup tapes shall be required by contract to ensure destruction in accordance with HIPAA compliant methodologies;
   b. Electronic media used for backup purposes or any temporary storage shall be controlled by the Chief Financial Officer and Liberty's Security Officer. All media shall be governed and managed by the following SOP provisions:

(i) CD's and other portable media storage devices only have the necessary data for someone to perform their job function - in general they shall be prohibited and require approval from a Liberty supervisor to utilize.

(ii) All portable media storage devices shall be physically secured by the individual using them and shall be destroyed by the IT group in a manner appropriate for the data retained and in a timely fashion;

(iii) Any data electronically transmitted to off-site locations shall utilize secure connection protocols such as SSL and other forms of data encryption;

(iv) Third party vendors maintaining Liberty data shall not be permitted to use it unless specified in contracts with the third party vendors. The contract provisions with third party vendors shall contain provision around securing the data and its use;

(v) The creation of backup jobs, job scheduling, and job processing shall be the responsibility of designated Liberty application owners;

(vi) Where possible, automated software shall be utilized to schedule, process, and monitor backup jobs;

(vii) Where possible, automated software shall be used to track data backups, backup media used to retain the data, and the physical location of the media. When automated solutions are not available, Liberty's Hiring Manager shall create and provide to Liberty's Security Officer a log sheet of all backup media, its contents, and physical location. Liberty's Hiring Manager and Liberty's Security Officer shall maintain such documentation at all times.

(viii) All backup media shall be maintained and stored in Liberty's data center until it is transferred to an off-site location;

(ix) All Liberty data shall be considered business confidential.

A – OFF-SITE STORAGE:

6. The Chief Financial Officer or Liberty's Security Officer or their designees shall be the only individuals who can authorize the movement of backup media to and from the off-site location OR to a location other than Liberty's data center:

   a. All media transferred to off-site locations shall be placed in secure containers identified by media labels indicating the contents are **Liberty Confidential Materials**;

   b. Only Liberty authorized personnel or the off-site storage vendor shall be allowed to transport media to and from the off-site location;

   c. All backup media stored off-site shall be inventoried by Liberty's Security Officer and the off-site location;

   d. Vendors providing off-site storage of electronic media shall maintain sufficient controls so that all of Liberty media shall be secure with the appropriate physical and environmental safeguards. Access to the media shall only granted to Liberty's Security Officer or their designee. Where possible these provisions are included in the contracts with the vendor;

   e. Liberty's Security Officer or their designee shall semi-annually perform an inspection of any vendors providing off-site storage services. At a minimum, the assessment includes the positive confirmation that the vendor shall maintain sufficient physical and environmental controls to protect Liberty media. Any potential weaknesses shall be brought to the vendor's attention and corrective action shall be pursued. Consideration of an SSAE 16 (Statement on Standards for Attestation Engagements No.16 – AICPA Attestation Standard) over the controls of the vendor shall be requested, but not necessarily required;

   f. Liberty's Security Officer or their designee shall semi-annually perform an assessment to confirm the Liberty's off-site inventory listing reconciles to the media possessed by the vendors. Any discrepancies shall be investigated and corrective action is pursued.

Regulatory References

45 C.F.R. 164.310(d)

Additional References

U.S. Department of Defense 5220.22-M Standards:

Sanitization is the process of removing sensitive information from a document or other medium, so that it may be distributed to a broader audience. When dealing with classified information, sanitization attempts to reduce the

document's classification level, possibly yielding an unclassified document. Originally, the term sanitization was applied to printed documents; it has since been extended to apply to computer media and the problem of data reminisce as well.

Redaction generally refers to the editing or blacking out of text in a document, or to the result of such an effort. It is intended to allow the selective disclosure of information in a document while keeping other parts of the document secret. Typically the result is a document that is suitable for publication, or for dissemination to others than the intended audience of the original document. For example, when a document is subpoenaed in a court case, information not specifically relevant to the case at hand is often redacted.

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:07:51 -05'00'

Return to Index

Liberty QualityCare® Liberty Healthcare Corporation HIPAA Standard Operating Procedure #25: Portable Computing Devices

Title:	**HIPAA – Portable Computing Devices**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	**01/23/2018**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall maintain specific protections and precautions for portable devices to reduce the potential exposure of Electronic Protected Health Information (ePHI).

PROCEDURE

1. Liberty shall maintain specific protections and precautions for portable devices to reduce the potential exposure of ePHI.
2. ePHI and other sensitive Liberty information cannot be stored on portable devices such as jump or USB/thumb drives, laptops, user's computer hard drives, compact discs or zip drives unless the Security Officer gives approval (JAS01/23/2018) and the device is encrypted, and the device is password protected.
3. Security precautions required of Liberty workforce members with Portable Computing devices include: (a) Using strong passwords - refer to Liberty's Standard Operating Procedure (SOP) "Workstation Use & Security"; (b) Portable computing devices are assigned to authorized Liberty workforce members ONLY; (c) Secure unattended portable computing devices; (d) Avoid using portable computing devices when possible.
4. Liberty workforce members using portable devices shall be required to be knowledgeable about the device's security features.
5. Liberty workforce members using portable devices shall report lost or stolen devices immediately to their supervisor, or to Liberty's Security Officer. Failure to take appropriate action to prevent theft or to report loss of a device is a serious offense and may result in termination.
6. Liberty workforce members are responsible for damage and/or loss or theft of portable computing devices. In order to avoid loss or theft: (a) Liberty devices shall not be left unattended; (b) Portable devices shall not be checked as luggage when travelling; (c) Diligence must be exercised when portable devices are passed through airport x-ray devices such that devices shall be tracked through the x-ray device and immediately collected as soon as permitted by airport security personnel; (d) Liberty devices shall be kept out of view when left in cars, however, to the extent possible, Liberty devices shall not be left unattended in an automobile; (e) Liberty devices shall not be stored in cars during very hot or very cold weather – temperature extremes can damage or destroy portable devices.
7. Non-company owned (visiting) devices, such as a Liberty workforce members personal devices shall not be connected into Liberty's Network without permission and assistance form Liberty's Security Officer or designee since it could be disruptive or destructive to Liberty's Network.

Regulatory References

45 C.F.R. 164.308(a)(4)
45 C.F.R. 164.312(d)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:08:21 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #26: Remote Access

Title:	**HIPAA – Remote Access**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall define procedures for connecting to Liberty's Network from remote locations outside the private network. The following procedures are designed to minimize the potential exposure to Liberty from threats that may result from unauthorized use of Liberty's resources or unauthorized exposure to Electronic Protected Health Information (ePHI). Liberty shall maintain secure mechanisms for remote access to ePHI.

PROCEDURE

1. Remote access to Liberty Systems or Networks with ePHI shall be granted only as necessary.
2. It shall be the responsibility of all Liberty workforce members with remote access privileges to Liberty's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Liberty.
3. If it is deemed appropriate that there is a need for business associate agreement between Liberty and the entity requesting remote access, the business agreement shall be in place before granting remote access.
4. Liberty workforce members shall be responsible to ensure that family members or household visitors do not gain access to the Liberty Network, its resources, or its data. The Liberty workforce member shall bear responsibility for any consequences should the access be misused or misappropriated.
5. Authorized remote Liberty workforce members shall not provide their login or password to anyone else, for any reason.
6. Authorized Liberty workforce members shall ensure that Liberty-owned or their personal computer or workstation, which is remotely connected to Liberty's Network, is not connected to any other network at the same time.
7. Authorized Liberty workforce members shall ensure Liberty –owned, or their personal computer or workstation, which is remotely connected to Liberty's Network, shall be protected with the latest Malware software protection before making connection to the Liberty Network.
8. Authorized remote Liberty workforce members shall NOT use non-Liberty email accounts (i.e. Hotmail, Yahoo, Google mail), or other external resources to conduct Liberty business, thereby ensuring that official business is never confused with personal business.
9. Routers for dedicated communication lines configured for access to the Liberty Network shall meet minimum authentication requirements of the Challenge Handshake Authentication Protocol (CHAP) (See Below for brief summary).
10. Frame Relay shall meet minimum authentication requirements of the Data Link Connection Identifier (DLCI) standards (Refer to the National Institute of Standards and Technology – NIST).
11. Non-Standard hardware configurations shall be approved by Liberty's Security Officer or designee. Liberty's Security Officer or designee shall approve security obligations for access to hardware. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Liberty Network in production SHALL obtain prior approval from Liberty's Security Officer or their designee. Remote Access information and Remote Access

Authorization forms SHALL be obtained from Liberty's Security Officer and completed by the remote access Liberty workforce member requester and approved by their Liberty supervisor. Both the Remote Access Information and Remote Access Authorization forms shall be returned to Liberty's Security Officer or their designee.

12. All authorized machines connected to Liberty's internal networks via remote access technologies shall use the most up-to-date anti-virus software.
13. All authorization shall be centrally managed by Liberty's Security Officer or designee and strong authorization measures shall be used.
14. Requestor's of remote access shall meet Liberty's minimum requirements for a related device to comply with Liberty's systems. Those who do not meet these requirements must upgrade their machines or face being denied remote access privileges.

CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password).[2]

1. After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
2. The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
4. At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.

Regulatory References

45 C.F.R. 164.308(a)(4)
45 C.F.R. 164.312(d)
National Institute of Standards and Technology (NIST) Firewalls and Firewall Policy

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:08:59 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #27: Access Control

Title:	**HIPAA – Access Control**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall implement technical Standard Operating Procedures (SPOs) for electronic systems that maintain Electronic Protected Health Information (ePHI) to allow access only to those persons or software programs that have been granted access to ePHI.

PROCEDURE

I. Unique User Identification:

1. All Liberty's workforce members with access to Liberty's Network containing ePHI through computer workstations shall be assigned a unique name and/or number for identifying and tracking user identity. Liberty's workforce members shall maintain their own passwords. Any software that uses ePHI shall require a Liberty assigned identification and user owned password (separate from the operating system identification and password). Refer to Liberty's Standard Operating Procedure (SOP) "Security Awareness and Training".
2. Liberty's workforce members shall be strictly prohibited from sharing identifications and passwords. Violations of this prohibition can result in sanctions up to and including termination as outlined in Liberty's SOP "Complaints, Sanction and Non-Retaliation.
3. Liberty's workforce member's identifications and passwords shall be monitored and maintained by Liberty's Security Officer or designee. Liberty's Security Officer or designee shall routinely audit to ensure that User rights remain appropriate given the Liberty job description of each Liberty workforce member. Refer to Liberty SOPs "Workforce Security" and "Security Awareness and Training".
4. Every Liberty workforce member shall log out of their workstation when not occupying it. This can be achieved by shutting down the workstation or logging off. Whichever method used, a user identification and password shall be required to gain re-entry.

II. Emergency Access Procedure:

5. All ePHI that is necessary for an emergency shall generally be retained by Liberty's workforce members and business associates and therefore communication with Liberty's workforce members and business associates in the time of an emergency shall cover all emergent situations. Liberty's Security Officer or designee shall work with Liberty's Executive Operations group to determine the nature of the emergency and together the action steps necessary to provide services in an emergency will be outlined.
6. The determination of who shall have emergency access, if any, shall be made collaboratively between Executive Operations, the Senior Vice President /Chief Operating Officer, the Chief Financial Officer and the Security Officer or their Designee.

III. Automatic Logoff:

7. Liberty's workforce members shall be required to provide a password to log into the system after 30 minutes of inactivity. In addition, Liberty's workforce members shall activate their workstation locking software whenever they leave their workstation unattended for any length of time.

IV. Encryption and Decryption:

8. Liberty's Security Officer shall implement a mechanism to encrypt and decrypt ePHI at rest.
9. All email incoming and outbound is key encrypted by encryption software. All Liberty workforce members shall have incoming and outbound email that is key encrypted by Liberty's encryption software. All senders and receivers of Liberty email with potential ePHI information shall have unique key encryption/decryption installed in their computer profile.
10. Whenever possible, all other ePHI shall be encrypted by Liberty's Security Officer or designee.
11. Valid encryption processes include those identified by the National Institute of Standards and Technology (NIST – See Below), other processes that are Federal Information Processing Standards (FIPS), or others that may be identified from time to time by the Secretary of Defense.

Regulatory References

45 C.F.R. 164.312(a)
74 Fed. Reg. 19006, 19008-10 (April 27, 2009)

National Institute of Standards and Technology (www.nist.gov) – Guide to Storage Encryption Technologies for End User Devices, NIST Special Publication 800-52, Guidelines for the Selection and Use of Transportation Layer Security (TLS) Implementations, 800-77, Guide to IPSec VPNs or 800-113

Federal Information Processing Standards (FIPS), 140-2

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:09:31 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #28: Audit Control

Title:	**HIPAA – Audit Control**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall implement hardware, software, and procedural auditing mechanisms to record and examine activity on information systems used by Liberty that contains or uses Electronic Protected Health Information (ePHI).

PROCEDURE

1. Liberty shall record and examine significant activity on information systems that it maintains or that are hosted by vendors that contain or use ePHI. Liberty has conducted a risk analysis to identify and define what constitutes "significant activity" on a specific information system. The most vulnerable of systems are maintained by business associates (except in conditions in which Liberty is the covered entity) and therefore, Liberty also relies on their obligations to monitor as well.
2. Appropriate hardware, software, or procedural auditing mechanisms shall be implemented on the information systems used by Liberty that contain or use ePHI.
3. The level and type of audit mechanisms implemented on information systems used by Liberty that contain or use ePHI shall be determined by Liberty's Chief Financial Officer, Liberty's Security Officer or designee and the risk analysis process.
4. Audit logs created by the audit mechanisms implemented on Liberty information systems shall be reviewed regularly. The frequency of such review is determined by Liberty's Security Officer or designees and the risk analysis process.
5. Liberty audit log review shall be performed by Liberty's Security Officer or designee.
6. When possible, Liberty's workforce members shall not review audit logs that pertain to their own system activity.
7. When possible, the real-time clocks of information system's used by Liberty shall be set to an agreed upon standard, military time, so that audit events are synchronized. Liberty shall have a procedure for monitoring and correcting any significant discrepancies in information system real-time clocks.

Regulatory References

45 C.F.R. 164.305(a)(5)(ii)(C)
45 C.F.R. 164.312(b)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:09:59 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #29:
Person or Entity Authentication

Title:	**HIPAA – Person or Entity Authentication**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	**12/21/2015**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall have an *authentication* mechanism in place to corroborate the authenticity of a person or entity prior to granting access to Electronic Protected Health Information (ePHI).

PROCEDURE

Passwords:

1. Liberty workforce members shall not share passwords with others. If a Liberty workforce member believes that someone else is inappropriately using a user-ID or password, they shall immediately notify their Liberty supervisor/manager. Liberty supervisors/managers shall not have access to subordinates' passwords and therefore shall report the Liberty workforce member's concern to Liberty's Security Officer or designee who shall ensure the potentially compromised password is reset.
2. Where possible, the initial password(s) issued to a new Liberty workforce member shall be valid only for the new user's first log-on to a workstation. At initial log-on, the Liberty workforce member shall be required to choose another password. Where possible, the same process shall be used when a Liberty workforce member's workstation is reset.
3. All passwords for high-risk ePHI shall automatically expire every 90 days. Passwords for low and medium-risk ePHI shall expire every 180 days. E.B. 12/14/15.
4. Passwords shall contain at least two of the following: an upper-case letter, a lower-case letter, a numeric digit (0-9) and a punctuation character such as (! <>*&^%$#).
5. Passwords shall not be based upon any personal information such as a user's first, middle, or last name, or a family member's name, date of birth or other identifying information. All password-based control systems on Liberty workstations shall mask, suppress, or otherwise obscure the passwords so that unauthorized persons are not able to discern them.
6. Passwords shall not be written down or stored anywhere in Liberty's program/facility or stored online except in an encrypted file with a password conforming to complexity criteria. E.B 12/21/15.
7. Users shall not use "Remember Password" features of any application (such as Netscape, Internet Explorer, Safari) when using a Liberty system password.
8. Liberty's Security Officer may attempt to password "crack" or guess a Liberty workforce member's password for purposes of ensuring passwords are sufficiently strong. If Liberty's Security Officer successfully "cracks" or guesses a user's password, the user shall be required to change the password immediately.

Authentication:

9. Liberty shall use appropriate authentication methods to confirm that only properly authenticated and authorized persons or entities' access ePHI: (a) Unique user identifiers (user Ids); (b) Security identifier (password); (c) Password systems; (d) Personal Identification Number (PIN) systems; (e) Security token Systems; (f) Biometrics identification systems; (g) Telephone callback systems; (h) Digital signatures.
10. Liberty's Authentication processes shall include but are not limited to: (a) Documented Standard Operating Procedures for granting persons and entities authentication credentials or for changing existing authentication methods; (b) Uniquely identifiable authentication identifiers in order to track the identifier to a Liberty workforce member; (c) Documented Standard Operating Procedures for detecting and responding to any person or entity attempting to access ePHI without proper authentication; (d) Removing or disabling authentication credentials in systems for persons or entities that no longer require access to ePHI; (e) Periodic validation that no redundant authentication credentials have been issued or are in use; (f) Protection of authentication credentials (i.e. Passwords, PINS)with appropriate controls to prevent unauthorized access; (g) When feasible, masking, suppressing, or otherwise obscuring the passwords and PINS of persons or entities seeking to access ePHI so that unauthorized persons are not able to observe them.
11. Access methods of authentication to ePHI Systems shall not be built into logon scripts. Exceptions shall be made only after review and approval by Liberty's Security Officer or designee.
12. Liberty shall limit authentication attempts to its ePHI to no more that the number of attempts reasonably determined by Liberty's Security Officer within a specified time. Authentication attempts that exceed the limit shall result, as appropriate, in: (a) Disabling the relevant account for an appropriate period of time; (b) Logging of event; (c) Notifying appropriate Liberty Executives.

Regulatory References
45 C.F.R. 164.312(d)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:10:31 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
Standard Operating Procedures #30:
Transmission Security

Title:	**HIPAA – Transmission Security**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	**09/24/2015**
Functional Area:	**ADMINISTRATION**		

POLICY

When sending Liberty ePHI over an electronic communication network, the ePHI shall be sent in encrypted form and shall have controls to safeguard the integrity of the data. The text and attachments of emails sent from Liberty corporate email accounts to other Liberty corporate emails accounts are encrypted in transmission. Such emails may contain PHI. (EB 09/24/2015) Further, at no time, should any Liberty workforce member utilize any email address other than their work email (i.e. no personal Gmail or Yahoo accounts

PROCEDURE

1. When sending Liberty ePHI over an electronic communication network, the ePHI shall be sent in encrypted form and shall have controls to safeguard the integrity of the data. The text and attachments of emails sent from Liberty corporate email accounts to other Liberty corporate emails accounts are encrypted in transmission. Such emails between Liberty corporate email accounts that are encrypted may contain PHI. Some non-Liberty corporate systems may support encryption in a way that emails, including attachments, sent between these systems and Liberty's corporate email system can be end-to-end encrypted. In these cases, PHI may be sent/received between these systems using encryption. In such cases, the Liberty Security Officer must determine that the cross-system encryption process is adequate and must periodically review to assure that the encryption features continue to operate. (EB 09/24/2015) Further, at no time, should any Liberty workforce member utilize any email address other than their work email (i.e. no personal Gmail or Yahoo accounts).
2. All transmissions including ePHI shall be sent via: (a) Virtual Private Network (VPN) connection that transmit ePHI shall utilize IPSec, SSL/TLS or SSH to establish temporary or permanent tunnels to the internal networks; (b) Ensuring proper authentication to access ePHI shall be accomplished through Mutual Authentication (in case of SSL/TLS or SSH tunnels) or Authentication header (in the case of IPSec tunnels); (c) Ensuing proper integrity of ePHI shall be accomplished by utilizing encryption with a symmetric session key (in the case of SSL/TLS or SSH tunnels); (d) Web applications shall utilize Secure Socket Layer (SSL) to ensure authentication and integrity of ePHI transferred over Hypertext Transfer Protocol (HTTP); (e) File Transfer Protocol (FTP) applications shall use either File Transfer Protocol –ES, SSL or Secure to ensure authentication and integrity of ePHI.
    a. When accessing ePHI through a remote connection, Liberty workforce members shall be required to use a secure Virtual Private Network (VPN) connection. ePHI accessed through a public wireless or Wi-Fi connection shall have a secure connection.
3. Encryption and integrity controls shall always be used when highly sensitive Liberty data such as ePHI and passwords are transmitted over electronic communications networks.
4. Liberty's integrity controls shall ensure that the value and state of all transmitted data is maintained and the data shall be protected from unauthorized modification. Such controls include check sums, message authentication codes, and hash values (hash values function is any algorithm that maps data of arbitrary length to data of a fixed length).

Regulatory References

45 C.F.R. 164.312(e)(1)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:11:03 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #31: Documentation Retention and Storage

Title:	**HIPAA – Documentation Retention and Storage**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall retain copies of all Standard Operating Procedures (SOPs) and all communications that are required to be in writing by HIPAA Privacy and Security Plan. Liberty shall also retain records of actions or designations that HIPAA requires to be documented. Materials will be maintained in written and electronic form and are maintained for six (6) years as part of the Corporate Compliance Program or when they were last in effect, whichever is later.

Procedure

Document Retention Checklist:

1. Liberty's Standard Operating Procedures (SOPs) for Privacy and Security Program.
2. HIPAA Person or Entity Authorizations.
3. HIPAA Program Amendments.
4. HIPAA Program Amendments Certifications.
5. Liberty Business Associate Agreements.
6. Notice of Privacy Practices of any patients/clients/persons Liberty serves.
7. Documentation that training has been provided to Liberty Employed and Subcontracted Staff (workforce members).
8. Data Use Agreements.
9. Information in Designated Record Sets to which individuals have access.
10. Complaints about Liberty's compliance with HIPAA rule, the HIPAA Privacy and Security Plan and their dispositions.
11. Documentation of sanctions applied to Liberty workforce members for violations of HIPAA or the HIPAA Privacy and Security Plan.
12. Notices that deny or delay an individual's access to their Protected Health Information (PHI).
13. Notices that deny or delay an individual's request to amend their PHI.
14. Disclosures of PHI for which a person is entitled to an accounting.
15. Written statements by agencies or officials supporting suspension of an accounting of PHI disclosures (including oral statements documented by Liberty).
16. Conclusions and supporting analysis from an expert that health information is de-identified.
17. Description of PHI disclosed.
18. Copy of disclosure requests.
19. Court Orders, Grand Jury Subpoenas, etc. where disclosures are required by law.
20. Written statements in connection with disclosures needed for other judicial/administrative processes, where the disclosure is not mandated by court order.
21. Copies of written accountings.
22. Liberty's notice of terminating a restriction on uses or disclosures of PHI previously agreed to by Liberty.
23. Individual's agreement or request to terminate a restriction on uses or disclosures of PHI previously agreed to by Liberty.

24. Other communications required by Liberty's Privacy and Security Plan to be in writing, including requests for Confidential Communications.

Procedure Steps:

25. Liberty shall document all necessary SOPs for HIPAA Privacy and Security Compliance and shall make all these SOPs for HIPAA Privacy and Security available to Liberty workforce members who deal with PHI in their work.
26. Liberty's Privacy Officer shall be responsible for receiving and processing access to PHI. Denial of access to PHI shall also be documented by Liberty's Privacy Officer.
27. Liberty's Privacy Officer shall be responsible for processing requests to amend PHI. Liberty's Privacy Officer shall also document any circumstances where amendment was denied.
28. All disclosures for purposes other than treatment, payment, health care operations, or in response to written authorizations shall be documented. Liberty's Privacy Officer shall be responsible to collect and store such documentation logs for audit purposes. Individual requests for restrictions to uses and disclosures of PHI shall be maintained by Liberty's Privacy Officer.
29. Liberty shall maintain documentation of training regarding privacy and security issues and shall document which Liberty workforce members have received such training and with what frequency.
30. Liberty's Vice President of Human Resources shall maintain documentation of terminations for Liberty workforce members for security violations.
31. Liberty's Privacy Officer shall document all circumstances where a patient/client has requested and received an accounting of disclosures of PHI.
32. Liberty's Legal Department shall maintain a file of business associate agreements and contracts.
33. Liberty's Security Officer shall keep documentation of the classifications of Liberty workforce members and their level of access to PHI.
34. Liberty's Privacy Officer shall maintain a file of complaints received and corrective actions taken.
35. Following the six (6) year maintenance term, paper documents shall be shredded.
36. Following the six (6) year maintenance term, Electronic records shall be deleted and all back up storage shall be erased and destroyed.

Regulatory References

45 C.F.R. 164.530(j)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:11:38 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #32:
Protection from Malicious Software

Title:	**HIPAA – Protection from Malicious Software**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall establish appropriate safeguards to protect Electronic Protected Health Information (ePHI), systems and other electronic information resources from known types of malicious software including viruses, worms, spyware, and Trojan Horses (Refer to the end of the SOP for further explanation). Liberty workforce members shall be trained in their role in employing these safeguards and in reporting anomalies.

Procedure

Personal Responsibility:

1. It shall be the continuing responsibility of all Liberty workforce members to use every precaution to ensure the protection of Liberty's computer, Network, and information assets from viruses, worms, and other forms of malicious software.

Software:

2. Liberty's Security Officer or designee shall equip all programmable Liberty workstations, except for diskless models with approved anti-virus software.
3. Liberty's Security Officer or designee shall provide and update the anti-virus for Liberty workstations.
4. Liberty's Security Officer or designee shall be responsible for ensuring that a current version of the anti-virus software is installed for all Liberty workstations.
5. Prior to use by Liberty workforce members, Liberty's Security Officer or designee shall properly screen all data, software, storage media, trial diskettes, and preconfigured systems obtained from sources external to Liberty to reduce the likelihood of contamination by computer viruses, worms, or other forms of malicious software. External sources include personally–owned PCs and workstations.
6. File servers shall run ant-virus checks continuously.

Anti-Spyware:

7. Anti-Spyware software shall be active on Liberty workstations at all times. Liberty shall provide anti-spyware software and updates to all its workstations.

A **Trojan horse**, or **Trojan**, in computing is a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the story of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece, because computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.

Regulatory References

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

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:12:11 -05'00'

Return to Index

Liberty QualityCare®
Liberty Healthcare Corporation
HIPAA Standard Operating Procedure #33: Change Control

Title:	**HIPAA – Change Control**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty shall use formal change control Standard Operating Procedures (SPOs) when implementing changes to its information systems. Change shall mean any alteration to a Liberty's information systems, infrastructure, or applications, and/or their configuration, other than basic administrative tasks that do not affect the security, confidentiality, integrity, or availability of electronic Protected Health Information (ePHI) on the information systems.

PROCEDURE

Security Officer Responsibilities:

1. When new systems are introduced, or changes are to be made to existing systems, a process of documentation, specification, testing, quality control, and managed implementation shall be created by Liberty's Security Officer or their designee.
2. Liberty's Security Officer or their designee shall ensure that all changes are properly analyzed, documented and communicated to those impacted by, or involved in their execution.
3. Changes shall be submitted to Liberty's Security Officer ONLY by Liberty workforce members who are authorized users.
4. Liberty's Security Officer or their designee shall track and store details of all changes.
5. Liberty's Security Officer or their designee shall perform a risk analysis prior to implementation to determine the potential impact of and need for any change.
6. Liberty's Security Officer or designee shall NOT implement any change without the change being properly planned, documented, reviewed, tested and approved.
7. Liberty's Security Officer shall complete system documentation upon completion of each change and updates the SOPs if necessary.

Submit Change Control Request:

8. The Liberty workforce members responsible for execution and implementation of a change shall prepare and submit a change request in writing to Liberty's Security Officer for approval before the change is effectuated.
9. The change request should:
   a. Identify the type of change:
      (i) Normal Change – allow the needed lead time to plan all aspects of implementation and follow the formal SOP "Change Control";
      (ii) Emergency Change – This is a change required to immediately restore service, avoid and outage, respond to a data incident or other immediate threat to the security, confidentiality, integrity or availability of information systems.
   b. Define the scope of the change:
      (i) Identify all systems impacted;
      (ii) Determine which business units or departments will be affected;
      (iii) Identify duration of any outages;

c. Describe the need for the change;
d. Identify risks:
   (i) Assess potential risks to security and integrity of systems including those involved in the maintenance or transmittal of Electronic Protected Health Information (ePHI);
   (ii) Determine whether any system security, such as firewalls, will need to be decreased or disabled in order to implement the change;
   (iii) Determine whether change implementation can occur in an environment segregated from systems that maintain or transmit ePHI for testing purposes before full implementation occurs;
e. Describe the change specifications, including:
   (i) Date, time and duration of change;
   (ii) A detailed testing plan;
   (iii) A detailed implementation plan;
   (iv) A detailed back out or recovery plan should the change fail or need to be abandoned;
   (v) Security measures that shall be utilized to ensure systems are not compromised during implementation.

Impact Assessment:

10. Upon receipt of a change request, Liberty's Security Officer or their designee shall perform a risk analysis as described in the SOP, "Security Management"
11. Liberty's Security Officer shall also consider:
    a. Who will the change affect?
       (i) Business units;
       (ii) Patients/Clients;
       (iii) Business Associates;
    b. What will the change affect?
       (i) Sites/locations;
       (ii) Systems availability ;
       (iii) Application availability;
       (iv) System security;
       (v) Processes and Practices;
12. Liberty's Security Officer shall consult with Liberty's Chief Financial Officer and others as needed, to ensure that each change is fully vetted and assessed before a determination is made on the change request.
13. Liberty's Security Officer shall fully document the risk analysis performed.

Approval or Rejection of Change Request:

14. Once Liberty's Security Officer or their designee shall conduct an impact assessment, including a risk assessment, Liberty's Security Officer shall approve or reject the change request.
15. Liberty's Security Officer or their designee shall be responsible for monitoring the implementation process for an approved change.

Implementation:

16. Liberty's Security Officer or their designee shall monitor and manage implementation of the change in accordance with the change specification, and ensure the implementation plan is properly followed.
17. Any deviations from the implementation plan shall be documented and assessed by Liberty's Security Officer for impact on the security, confidentiality, integrity and availability of Liberty's information systems.
18. Once the change has been executed, the Liberty information systems shall be evaluated to ensure they have not been compromised and that all physical and technical safeguards remain active.

Emergency Changes:

19. Emergency changes necessitated by a system failure, outage or other incident requiring immediate response shall be executed without the completion of the formal change request process. However, Liberty's Security Officer shall be notified and must approve any emergency change. Should Liberty's Security Officer not be available, the Chief Financial Officer shall approve the emergency change.

20. Following implementation of any emergency change, a change request shall be completed and documented by Liberty's Security Officer. Liberty's Security Officer shall also conduct a risk analysis to assess the impact on ePHI and shall ensure that the security, confidentiality, integrity and availability of the information system shall not been compromised.

Documentation:

21. Liberty's Security Officer shall maintain the following documentation regarding all changes:
    a. A copy of all change requests submitted and their disposition;
    b. Documentation of the risk analysis and its result for each approved change request;
    c. Documentation of the implementation of the change and any associated audit logs.
22. Liberty's Security Officer shall also ensure that all system and user documentation, and any associated SOPs are updated to reflect the change.

A **Trojan horse**, or **Trojan**, in computing is a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the story of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece, because computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.

Regulatory References
45 C.F.R. 164.308

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:12:47 -05'00'

Return to Index

Liberty QualityCare® Liberty Healthcare Corporation HIPAA Standard Operating Procedure #34: Breach Notification

Title:	**HIPAA – Breach Notification**	**Effective Date:**	**10/03/2014**
Author:	**Security Officer**	**Last Review Date:**	**12/20/2018**
Location:	**All Locations**	**Last Revision Date:**	**01/23/2018**
Functional Area:	**ADMINISTRATION**		

POLICY

In the event of impermissible access, acquisition, use or disclosure of Protected Health Information (PHI) in violation of 45 C.F.R. 164414 (d), Liberty as a covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications and other actions – revised JAS 08/20/2015 were made as required by the law.

PROCEDURE

1. Liberty workforce members shall notify their direct chain of command up to and including the Vice President of Operations and the Privacy Officer of any known or suspected breach or data incident for-JAS01/23/2018 disclosure of PHI.
2. Liberty's Vice President of Operations shall notify their direct chain of command, following their investigation of the data incident or-JAS01232018 or breach.
3. Liberty's Vice President of Operations shall notify the covered entity of the breach at the time of their notification.
4. Liberty's Privacy Officer shall notify General Counsel with the following information:
    a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    b. The unauthorized person who used the PHI or to whom the disclosure was made;
    c. Whether the protected health information was actually viewed (if known);
    d. The extent to which the risk to the subject of the PHI from the data incident or JAS 01/23/2018 or breach has been mitigated - revised 08/07/2015
5. General Counsel in collaboration with the Senior Vice President, Vice President of Operations, Liberty's Privacy Officer and /or Liberty's Security Officer shall determine if the definition of breach was met.
6. The covered entity shall have the burden of going forward and the burden of persuasion with respect to notifications of a breach.
7. If Liberty as a covered entity or a business associate knows of an impermissible use or disclosure of PHI, Liberty's Privacy Officer shall maintain documentation of all required notifications made, or alternatively of its risk assessment or the application of any exceptions to the definition of "breach" to demonstrate that notification was not required.

Regulatory References

45 C.F.R. 164.414 (d)

Approved By: Judith Ann Shields

Digitally signed by Judith Ann Shields
DN: cn=Judith Ann Shields, o=Liberty Healthcare Corporation, ou=Competency Evaluation, email=judiths@libertyhealth.com, c=US
Date: 2019.01.17 14:13:22 -05'00'

Return to Index