Liberty Healthcare Corporation
THE FREEDOM TO SUCCEED™

Standard Operating Policies - SOP # 1: HIPAA Privacy Compliance Program Overview

Title:	**HIPAA Privacy Compliance Program Overview**	Effective Date:	**10/03/2014**
Author:	**Privacy Officer**	Last Review Date:	**12/01/2021**
Location:	**All Locations**	Last Revision Date:	**12/01/2021**
Functional Area:	**ADMINISTRATION**		

POLICY

Liberty Healthcare Corporation, and all of its Affiliates (collectively "Liberty") conduct various operations in most cases make it a "Business Associate" and sometimes a "covered entity" as defined by the Health Insurance Portability and Accountability Act of 1996 .

In the course of its day to day operations, Liberty uses and discloses protected health information ("PHI") of Covered Entity clients. In recognition of its obligation to protect patient information, Liberty protects the confidentiality, availability, integrity and privacy of PHI in accordance with federal and state law, including but not limited to the Health Insurance Portability and Accountability Act of 1996 and its 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").

To comply with HIPAA, Liberty shall engage in a variety of activities that are an integral part of the Liberty HIPAA Privacy Compliance Program (Program). The Program SOPs are applicable to Liberty as defined above as well as all members of the Liberty Workforce (employees and subcontracted workforce).

Liberty uses and discloses PHI on behalf of its Covered Entity clients as a Business Associate to provide services for those clients. Liberty uses and discloses PHI on behalf of clients for payment and health care operations purposes. Liberty also may use and disclose PHI for treatment on behalf of Covered Entity clients but may not submit any FPHI in standard electronic form in connection with a HIPAA covered transaction.

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 Liberty subcontractors in their contracts with Liberty.

There are many terms which are capitalized in these HIPAA Standard Operating Policies. Please consult HIPAA for definitions of capitalized terms.

PROCEDURE

Privacy Rule: To comply with the Privacy Rule, Liberty shall require annual Liberty Workforce training on the HIPAA rules and shall develop a complaint process in the Program so that Liberty's Workforce members can file complaints regarding policies, practices, and compliance with HIPAA. The Program includes standard operating procedures for disciplinary actions and terminations for Liberty's Workforce members who violate the 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 Policies ("SOPs"). 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 electronic PHI ("ePHI"). Liberty shall implement reasonable administrative, physical and technical safeguards to

protect ePHI (45 C.F.R 164.306(a)). Liberty shall perform annual security risk assessments. Liberty shall annually evaluate the HIPAA Security SOPs in light of existing threats and new technologies. In addition, an additional 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, HIPAA was 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. Notification to clients will be determined by their specific contract with Liberty. A breach is the unauthorized "access, acquisition, use or disclosure" of PHI. Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified under HIPAA guidance. Liberty shall have an explicit 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 and have different rules for notification. HIPAA has two (2) main rules relating to how it intersects with state law. FIRST, state laws that are contrary to HIPAA are preempted by HIPAA, which mean HIPAA applies (45 C.F.R. 160.202). SECOND, when a state law is more stringent than HIPAA, Liberty shall abide by the more stringent regulation or statute.

State Law: State Data Breach Laws: As of this review, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation for 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 PHI, the incident shall still be evaluated by Liberty's Chief Compliance Officer for notification requirements under existing state laws.

Approved By: John G. Beck Digitally signed by John G. Beck Date: 2022.01.10 14:05:50 -05'00'

Revision History

Version	Date	Author	Summary of Changes
#1	10/03/2014	Judith Ann Shields	Initial ISF release – refactor and update of previous security policies into distinct documents
#2	12/22/2015	Judith Ann Shields	Annual review, Attorney reviewed added ePHI. Added inactivity lock requirement
#3	12/22/2016	Judith Ann Shields	Annual review, Attorney reviewed no changes. Added inactivity lock requirement
#4	12/22/2017	Judith Ann Shields	Annual review, Attorney reviewed no changes. Added inactivity lock requirement
#5	12/22/2018	Judith Ann Shields	Annual review, Attorney reviewed no changes. Added inactivity lock requirement
#6	12/22/2019	Judith Ann Shields	Annual review, Attorney reviewed no changes. Added inactivity lock requirement
#7	11/02/2020	Judith Ann Shields	Annual review, Attorney reviewed Policy Title change. Added inactivity lock requirement
#8	12/01/2021	John Beck	Annual review, Attorney reviewed and made substantial changes to policy. Added inactivity lock requirement