




Policies and Procedures:

SECURE USE AND TRANSMISSION OF ELECTRONIC PROTECTED HEALTH INFORMATION

<input checked="" type="checkbox"/> MEDICAID	<input checked="" type="checkbox"/> DUALS	<input checked="" type="checkbox"/> MEDICARE	<input checked="" type="checkbox"/> COMMERCIAL
Responsible Department: Compliance		Approved By: Peter Fuentes, DMD Chief Dental Officer  Kristina Rovirosa Vice President <i>Kristina Rovirosa, RN, BSN</i> Quality Management	
Issue Date: 12/17/2002		Approval Date: 11/30/2021	

PURPOSE/SCOPE:

Consistent with 45 CFR §164.306(a) and §164.312(e)(1), the purpose of this policy is to:

1. Safeguard the confidentiality of electronic protected health information (e-PHI) LIBERTY Dental Plan Corporation, its affiliates and subsidiaries (collectively, “LIBERTY”), receive, or transmit;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information when transmitted to or from LIBERTY;
3. Protect against any reasonably anticipated uses or disclosures of such information when transmitted to or from LIBERTY that are not permitted under applicable law or contract;
4. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network; and
5. Promote compliance with this policy among LIBERTY’s employees, contractors and participating providers (collectively, “LIBERTY Personnel”).

This policy applies to all LIBERTY lines of business, including those in which LIBERTY’s role is Covered Entity and those in which its role is Business Associate, and to all LIBERTY Personnel.

DEFINITIONS:

HIPAA Privacy & Security Rules	Unless otherwise specified herein, the terms used within this policy shall have the same meaning as defined under the HIPAA Privacy Rule at 45 CFR § 160.103 and the Security Rule at 45 CFR § 164.304.
LIBERTY Personnel	For purposes of this policy, the term “LIBERTY Personnel” shall include LIBERTY employees, contractors with access to LIBERTY PHI, and participating providers.

POLICY:

1. LIBERTY Personnel shall use only the following methods to transmit LIBERTY PHI electronically, provided that only the minimum necessary PHI to complete the required purpose is used or disclosed, and the use or disclosure is permitted under applicable law and contract:
 - a. Secure Fax;
 - b. Secure File Transfer Protocol (SFTP);
 - c. Secure internal systems or drives;
 - d. For LIBERTY employees:
 - i. LIBERTY email for internal communications
 - ii. **Encrypted** LIBERTY email for external communications
 - e. For LIBERTY participating providers and contractors,
 - i. LIBERTY's secure email portal; or
 - ii. Provider's or contractor's own secure, HIPAA-compliant email which includes encryption to prevent unauthorized access to e-PHI and requires recipient's authentication when sent through open internet.
2. LIBERTY Personnel shall not store, access or transmit PHI outside of the United States, or while outside of the United States.
3. When LIBERTY Personnel transmit a member's own PHI to the member, however, LIBERTY Personnel may honor the member's written request to receive the PHI electronically through a method other than those listed above, provided that LIBERTY Personnel has taken reasonable steps to validate the member's identity, and has disclosed to the member in writing the potentially unsecure nature of the transmission.
4. When LIBERTY requests PHI from external parties, the request shall clearly specify the permissible methods by which such PHI may be submitted electronically to LIBERTY, consistent with those listed above.
5. Immediately upon becoming aware of any potential or actual electronic transmission of LIBERTY PHI using a method other than those listed above, LIBERTY Personnel shall report such transmission via LIBERTY's Incident Management System ("IMS"), LIBERTY's dedicated IMS mailbox: ims@libertdentalplan.com, or LIBERTY's Compliance Hotline.

PROCESS/PROCEDURE

LIBERTY Personnel shall transmit e-PHI as follows:

1. Internal email, systems or drives

- a. Information transmitted within internal email, systems, or shared drives may contain PHI that is limited to the use and disclosure of the minimum necessary data to complete the required purpose.
- b. PHI (e.g., Member name, Social Security Number, Member Identification Number) shall not be included in the subject line of emails or file names.

- c. PHI shall not be saved to computer desktops (local hard drives), nor shall PHI (or sensitive PII) be entered into companywide platforms such as Compliance Central or CRTS in a screen or field that is openly viewable to users.
- d. LIBERTY Personnel shall not transmit PHI via phone text message, except as part of an approved member texting campaign.
- e. LIBERTY Personnel shall not transmit PHI to personal devices including as personal phone text messages; personal computers, personal email.
- f. LIBERTY Personnel shall not photograph, or video or audio record any area within LIBERTY without express written consent from Director level or above.

2. External email, systems or drives

- a. Email sent through the open internet shall be Encrypted to prevent unauthorized access to PHI and may contain PHI that is limited to the use and disclosure of the minimum Necessary data to complete the required purpose consistent with Policy Item #1 above.
- b. LIBERTY Personnel shall not save or store data files that contain PHI in an electronic format on public or private computers, unencrypted personal removable storage devices, personal cloud storage, and/or personal email accounts.
- c. LIBERTY Personnel shall not transmit LIBERTY PHI via public internet networks (such as airport; coffee shops; restaurants; etc.) or via phone text message, except as part of a LIBERTY approved member texting campaign, or upon member's written request, consistent Policy Item #2 above.

3. Training

- a. Employees - upon hire, and annually thereafter, all employees shall receive, acknowledge and complete training regarding this policy.
- b. Participating Providers- all Provider Manuals shall include a section setting forth Electronic Transmission of PHI requirements for providers, consistent with this policy. All provider contracts shall include a provision requiring the provider to comply with applicable state and federal privacy and security requirements including, but not limited to, HIPAA.
- c. Contractors – all contractors who have access to LIBERTY PHI shall enter into a Business Associate Agreement with LIBERTY and shall receive, acknowledge and attest to their compliance with this policy upon contracting with LIBERTY, and annually thereafter.