2.3.5 Secured Electronic Transmittal of Protected Health Information

(a) Policy

California Correctional Health Care Services (CCHCS) Health Information Management (HIM) and Health Records shall send Protected Health Information (PHI) in compliance with applicable federal and state privacy and security related regulations and laws.

(b) Purpose

To ensure patient confidentiality and privacy protection while sending health related documentation via the designated shared drive, and to ensure disclosures of PHI are documented (e.g., Right to Accounting of Disclosures of PHI).

(c) Policy Responsibility

(1) Under the direction of the Deputy Director, Medical Services, HIM Headquarters, Institution Health Records, and Health Record Center (HRC) staff are responsible for the oversight, implementation, monitoring, and evaluation of this policy.

(2) The Chief Executive Officer, or designee, Health Records Technician III (HRT III), and Health Record Technician II (HRT II) of each institution are responsible for the implementation, monitoring, and evaluation of this policy.

(d) Procedure Overview

CCHCS HIM and Health Records shall ensure patient PHI via the designated file transfer protocol.

(e) Procedure Responsibility

(1) Under the direction of the Deputy Director, Medical Services, HIM Headquarters staff are responsible for the oversight, implementation, monitoring, and evaluation of this procedure.

(2) The Chief Executive Officer, or designee, HRT III, and HRT II of each institution are responsible for ensuring all PHI is transmitted electronically by a method that is safe, secure, and complies with federal and state guidelines.

(f) Procedure

(1) External Party Access Request

When an External Party requests access to PHI, a Data Transfer Agreement must first be signed by both CCHCS and representatives of the External Party.

(2) Institution Designated Secure File Transfer Protocol Process

(A) Received Release of Information (ROI) requests shall be logged into the ROI tracking mechanism by California Department of Corrections and Rehabilitation (CDCR) number, patient name, date received, number of pages uploaded, and date uploaded/completed.

(B) The signed ROI request shall be scanned into the health record.

(3) Creating an Encrypted Document File

Identify documents within the health record that have been requested.

(A) Combine the requested documents into a single file.

(B) Prepare the encrypted document for transmittal.

(C) Transmit encrypted document using the approved delivery method.

(4) Shared File Upload Process

(A) Documents shall be compiled and saved onto a designated shared folder.

(B) All files shall be saved by using a formal naming convention as specified by HRC.

(C) The user is prompted to create a State compliant password when saving the file.

(D) The files shall be uploaded to the designated shared drive.

(E) Files shall be routed to the designated county according to the specified County Code.

(F) After verifying the upload is successful, the request shall be logged as completed.

(G) The uploaded files shall remain on the designated shared drive for 30 calendar days.

(H) The County Mental Health Department shall retrieve the documents from the designated shared drive.

(5) Facsimile

(A) Cover Sheet

1. Attach the cover sheet to all facsimile correspondence as the first page.
2. Include the following two statements on the cover sheet:
   a. “Transmittal is Confidential.”
   b. “If the information transmitted is received by someone other than the intended individual, the sender shall be immediately notified.”

(B) Transmittal and Post Transmittal Verification

When documents are sent by facsimile, the sender shall:

1. Phone the recipient to verify the recipient's name and facsimile number and inform him/her of the imminent transmission.
2. Ask that the recipient stay near the facsimile machine to intercept the documents.
3. Verify receipt of health care information by reviewing the print-out from the facsimile machine. Contact the recipient to verify documents were received.
4. Verify with the recipient that all documents were received and document this verification.
5. Review documents for completeness and legibility.
6. Be notified if all or part of the document must be retransmitted.

(C) Facsimile Log

Record all facsimile transmissions into the Facsimile Log and include:

1. The name, address, and telephone number of the sending and/or receiving entities.
2. The name of the patient and CDCR number.
3. The number of pages sent and/or received.
4. The date of transmittal.
5. Receipt received or requested.

(D) Misdirected facsimile tracking

1. Verify the information with the internal log (i.e., facsimile number, recipient name).
2. Contact the recipient via telephone or facsimile to explain the misdirection.
    a. Request the destruction or return of all documents sent via facsimile in error.
    b. Record the response on the facsimile cover letter and in the Facsimile Log.
    c. Follow the CCHCS Security Incident Reporting Procedures.

References

- Code of Federal Regulations, Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Health Care Department Operations Manual, Chapter 2, Article 2, Confidentiality and Privacy
- California Hospital Association Consent Manual, Chapter 15-17, *A Reference for Consent and Related Health Care Law* (37th ed., 2010)

Revision History

Effective: 01/2002
Revised: 08/2016