

DATA TRANSMISSION SECURITY

The appropriate measure of transmission security necessary is determined through the risk assessment process and outlined in the Facility Master Security Management Report.

1. The Departmental Information Security Officer (DISO) or his/her designee must ensure that DMH deploy and maintain integrity controls and encryption to protect Protected Health Information (PHI) and other confidential communications transmissions over the Internet, external connections, and all parts of the communications network (i.e., Local and Wide Area Network or LAN and WAN).
2. The DISO will provide oversight and guidance to the Department of Mental Health Chief Information Officer (DMH CIO) or his/her designee to deploy the appropriate network security methods stated in the DMH Network Security Architecture and the DMH IT Network Security Guidelines.
3. The DMH CIO or his/her designee must ensure that the facility LAN is optimally managed, operational, secured, and integrates into the DMH WAN for secured Internet and external connections.
4. The DMH CIO or his/her designee must ensure that the System Managers/Owners utilize and maintain integrity controls and encryption whenever deemed appropriate to protect PHI and other confidential communications transmissions.
5. The DMH CIO or his/her designee must ensure that the System Managers/Owners take into consideration each system's Risk Analysis Sensitivity Score (DMH Policy No. 550.01, Security Management Process: Risk Management), implement controls to ensure only authorized workforce members have access to network services for secured data transmission (DMH Policy No. 554.02, System Access Control Policy).
6. The DMH CIO or his/her designee must ensure that the integrity controls and encryption implemented under this policy are documented within the System Security Documentation (DMH Policy No. 554.02, System Access Control Policy: Definitions).
7. The DMH CIO or his/her designee must ensure that the System Managers/Owners implement the following integrity control procedures:
 - a. Identify the information communicated across networks, including all traffic containing PHI and other confidential information, for which data integrity will be checked.

- b. Determine the integrity controls (e.g., application or network message authentication tools) that will be used to perform the integrity inspections.
 - c. Utilize the selected integrity controls to check the integrity of incoming PHI and other confidential messages.
 - d. If the tool reports a discrepancy between the message received and the message sent, or if it appears that no message authentication measure has been included, then the System Managers/Owners must notify the DMH CIO or his/her designee.
8. The DMH CIO or his/her designee must ensure that the System Managers/Owners implement the following encryption procedures when deemed necessary pursuant to the DMH Risk Management Plan:
- a. Determine the encryption mechanisms that will be used in transmitting or receiving PHI and other confidential information messages over an open communications network and ensure that such encryption mechanisms are compatible with the encryption features employed by entities with which the facility communicates.
 - b. PHI and other confidential messages requiring encryption must be encrypted at the application or network layer prior to being transmitted.
 - c. Ensure that the passwords, tokens, and keys associated with the message encryption measures are protected from unauthorized disclosure or access as according to DMH Policy 554.02, System Access Control Policy: Encryption and Decryption Procedures.