MISSISSIPPI DIVISION OF MEDICAID

Encryption Policy

Policy #: 18.2

Approved By: Sheila Kearney, CSIO

Original Internal iTECH Effective Date: June 1, 2014
Effective Date for All Employees: September 28, 2017

Purpose:
The purpose is to ensure the encryption of confidential information while in transit.

Scope:
This policy applies to all DOM workforce members and anyone else granted access to DOM assets, resources, and/or confidential data. This policy also applies to all systems, networks, and applications, as well as all entities, which process, store, transmit, or maintain confidential information.

Policy:
DOM uses encryption to maintain the security and integrity of confidential information being transmitted over a network.

Procedure(s):

A. All transmissions of confidential information from the DOM network to a network outside of the DOM network must utilize an encryption mechanism between the sending and receiving entities or the file, document, or folder containing said confidential information must be encrypted before transmission.
B. The transmission of confidential information from DOM to a beneficiary via an email is permitted if the sender has ensured that the following conditions are met:

    1. The beneficiary has been made fully aware of the risks associated with transmitting confidential information via email.
    2. The beneficiary has formally authorized DOM to utilize an email to transmit confidential information to them.
    3. The beneficiary's identity has been authenticated.

C. When transmitting confidential information via removable media, including but not limited to, CD-ROM, memory cards, magnetic tape, solid state drives, and hard drives, the sender must:

    1. Use an encryption mechanism to protect against unauthorized access or modification.
    2. Authenticate the person or entity requesting said confidential information in accordance with Policy #17.1, Person or Entity Authentication Policy.
    3. Send the minimum amount of said confidential information required by the receiving person or entity.
    4. Route all requests from outside the agency for confidential information in accordance with Requests for Information standard operating procedures.

D. The transmission of confidential information over DOM's wireless network is permitted if the following conditions are met:

    1. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized.
    2. The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network.

E. If transmitting confidential information over a wireless network that is not utilizing an authentication and encryption mechanism, the confidential information must be encrypted before transmission.

F. The authentication and encryption security mechanisms implemented on wireless networks within DOM are only effective within those networks. When transmitting outside of those wireless networks, additional and appropriate security measures are utilized.

Responsibilities:
All workforce members are responsible for:
- Understanding and following all security related policies and procedures related to encryption.

The Security Officer (SO) is responsible for:
- Ensuring adherence of the Encryption Policy.

Retention:
Every policy and procedure revision/replacement will be maintained for a minimum of six years from the date of its creation or when it was last in effect, whichever is later. This policy preempts any retention policy which may require a shorter period.

Compliance:
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Form(s): None

References:
- Omnibus HIPAA Final Rulemaking, http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html
- International Standards Organization (ISO 27002).
- HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/, February 20, 2003.
- American Reinvestment and Recovery Act of 2009 (ARRA)/(HITECH). http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf. *(The HITECH Act begins at H.R. 1-112 through 1-165 (pp. 112 through 165 in the document). The security and privacy provisions are found at Subtitle D Privacy, beginning H.R. 1-144 (p. 144)).*
- NIST 800-113, Guide to SSL VPNs, http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf.
- NIST 800-77, Guide to IPsec VPSs, http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf.
- NIST 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf.
- Health Information Privacy, Security, and Your EHR http://www.healthit.gov/providers-professionals/ehr-privacy-security
- Achieve Meaningful Use: Protect Electronic Health Information http://www.healthit.gov/providers-professionals/achieve-meaningful-use/core-measures/protect-electronic-health-information http://www.healthit.gov/providers-professionals/achieve-meaningful-use/core-measures-2/protect-electronic-health-information

Contact:
Keith Robinson, Security Officer
550 High Street, Suite 1000
Jackson, Mississippi 39202

E: Thomas.Robinson@medicaid.ms.gov
P: (601) 359-6405
F: (601) 359-6294

Policy History: Original Internal iTECH effective date: June 1, 2014
Revised/Reviewed: March 15, 2016
Revised/Reviewed: September 18, 2017
Effective Date for All Employees: September 28, 2017