MISSISSIPPI DIVISION OF
MEDICAID

Transmission Security Policy

Policy #: 18.1

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 guard against unauthorized access to confidential information that is being transmitted over an electronic communications network.

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 facilities, which process, store, maintain, or transmit confidential information.

Policy:
DOM follows NIST guidelines for Integrity Controls and Encryption Implementation whenever possible and appropriate.

Procedure(s):
DOM follows NIST Special Publications 800-52, 800-77, and 800-113 to protect the integrity of data in motion.

Responsibilities:
The Security Officer is responsible for adherence to the Transmission Security 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