MISSISSIPPI DIVISION OF MEDICAID

Integrity Controls Policy

Policy #: ECP-411

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 that the integrity of electronically transmitted confidential information is properly maintained until disposed.

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 maintains controls to ensure the integrity of information transmitted over the network infrastructure and that confidential information is properly maintained until disposed of by an authorized member of the workforce.

Procedure(s):

A. DOM must authenticate the receiving person or entity prior to transmission of confidential information from the DOM network to a network outside of the DOM network.

B. DOM should only include the minimum amount of confidential information as determined by the Privacy Officer when transmitting to a network outside of the DOM network.

C. The transmission of confidential information from DOM to an outside entity via email is permitted if the sender has ensured that the following conditions are met:

    1. The receiving entity has been authenticated.
    2. The sender and receiver are able to implement a compatible encryption mechanism.
    3. All messages containing confidential information are encrypted.

D. Removable media for the purpose of system backups and disaster recovery is stored and transported securely.

E. The transmission of confidential information within DOM via an email is permitted without additional security measures or safeguards so long as only a minimal amount of confidential information is being transmitted.

Responsibilities:
The Security Officer will be responsible for ensuring the adherence to the Integrity Controls 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.

2016 | © All Rights Reserved | DOM https://www.medicaid.ms.gov/

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)).*
- 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: Initial 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