MISSISSIPPI DIVISION OF
MEDICAID

Encryption and Decryption Policy

Policy #: 14.4

Approved By: Sheila Kearney, CSIO

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

Purpose:
The policy specifies DOM's encryption and decryption requirements for protecting confidential information.

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, maintain, or transmit confidential information.

Policy:
Confidential information must be protected by data encryption. For confidential information that is stored on media which cannot be protected by encryption, other methods of access control must be utilized. Encryption and Decryption will be utilized in combination with other access controls where indicated by risk analysis.

Procedure(s):

A. Network Management Staff (NMS) makes use of a VPN and/or SSL connection between all remote computers back to the DOM network.

B. NMS utilizes secure web-servers for remote access to the DOM network which includes applications and email.

C. DOM uses standard algorithms for encryption technologies and will continue to evaluate new technology as it becomes available for transmitting confidential information outside its trusted network.

- DOM key length requirements will be reviewed annually and upgraded as technology emerges. All keys generated will be stored at a secure location for retrieval in an emergency.
- The use of proprietary encryption algorithms is not allowed for any purpose, unless approved by the Security Officer (SO).

D. NMS ensures that all critical data files are kept in read only format wherever possible and that the fewest number of individuals possible have access to modify these files.

E. iTECH ensures that all data transmissions to the Fiscal Agent are done through a secure transmission protocol.

F. DOM utilizes digital certificates or other accepted authentication methods when exchanging confidential information with outside entities.

G. DOM tests encryption and decryption capabilities of products and systems to ensure proper functionality.

Responsibilities:
The SO is responsible for ensuring adherence to the Encryption and Decryption 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 800-111, Guide to Storage Encryption Technologies for End Users, http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.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