DEPARTMENT OF ADMINISTRATION
Enterprise Policy

HR-HIPPA CONFIDENTIALITY-2015

DIVISION OF HUMAN RESOURCES

HIPPA Confidentiality Policy

Date of Last Revision 06/18/2015

Mike Sligar
(401) 574-8535
mike.sligar@hr.ri.gov

1. **Policy**

   a. The Rhode Island Department of Administration ("DOA") administers the State employee health plan in accordance with R.I. Gen. Laws §§ 36-12-2 and 36-12-6. Therefore, DOA is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (as amended) ("HIP AA") and must provide confidentiality protections for any individually identifiable health information ("PHI" or "protected health information") it maintains or has access to.

   b. DOA has designated itself as a "Hybrid Entity" in accordance with HIPAA. See Department of Administration's Designation as a Hybrid Entity under HIPAA, DOA-HIPAA-1. The health care components of DOA shall operate in conformance with the administrative, physical and technological requirements of HIP AA, the Genetic Information Nondiscrimination Act of 2008 ("GINA") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009, and regulations promulgated thereunder, including, but not limited to, the "Omnibus Rule" at 78 Fed. Reg. 5565 (Jan. 25, 2013).[1]

   c. DOA shall at all times have a named Privacy Officer and a named Security Officer appointed by the DOA Director. The DOA HIPAA Privacy and Security Officers are authorized to promulgate new procedures and amend existing procedures to effectuate DOA's conformance with HIPAA, GINA, HITECH and the regulations promulgated thereunder, including, but not limited to, the Omnibus Rule.

   d. A DOA employee's failure to comply with this HIPAA Confidentiality Policy or any of its underlying procedures may result in corrective disciplinary action up to, and including, termination of employment.

   e. This policy and its underlying procedures may be amended or rescinded without notice.

2. **Procedures**

   a. DOA is responsible for administering the State employee health plan. To accomplish this responsibility, it contracts .with a third-party administrator ("TPA") that processes claims and coordinates payments. As such, the TP A maintains detailed records with respect to a participant's visits to medical providers and the claims and payments arising from those

[1] Modifications to the HIP AA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIP AA Rules; Final Rule, 78 Fed. Reg. 5565 (Jan. 25, 2013) (amending 45 C.F.R. Parts 160 and 164). Available athttp://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073 .pdf.

visits. DOA only maintains limited protected health information ("PHI"), primarily consisting of enrollment information, coverage elections, and basic confidential information such as social security number and date of birth. Medical providers (diagnosis & treatment information) and/or the State's TPA (claims and payment information) maintain more expansive PHI traditionally understood as private medical information. Nonetheless, as an administrator of a health plan, DOA is obligated to maintain confidentiality of any PHI it maintains or has access to.

b. For purposes of these procedures, the following non-exhaustive list of information is PHI when considered in relation to the State employee health plan: name, address, telephone number, fax number, email address, social security number, health plan identification number, and any other unique identification number, characteristic or code relating to an individual. A disclosure of PHI is the release, transfer, provision of access to, or divulging of PHI in any manner to someone or something outside of the DOA health care components. Unless otherwise indicated, all references to employees are restricted to employees of DOA health care components.

3. Disclosures of PHI

a. Employees shall never disclose PHI unless:

(i.) The PHI disclosed is of the person requesting its disclosure.

(ii.) The disclosure is authorized by the individual pursuant to a HIPAA-compliant authorization, in a form provided by the Privacy Officer.

(iii.) The disclosure is to or among Office of Employee Benefits ("OEB") personnel for the purpose to administering health plan coverage or responding to inquiries from authorized persons.

(iv.) The disclosure is for treatment purposes: for instance, to qualified professionals who have medical or psychological responsibility for the care of an employee, retiree or dependent.

(v.) The disclosure is for payment purposes: for instance, to a third party administrator or other person or organization in connection with processing a claim the payment of which an employee, retiree or dependent may be entitled to.

(vi.) The disclosure is for DOA health care operations: for instance, to DOA business associates with valid business associate agreements.[2]

(vii.) The disclosure is to the federal Department of Health and Human Services for HIPAA compliance investigation, upon presentation of proper representation.

(viii.) The disclosure relates to compliance with worker's compensation laws.

[2] A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. HIPAA allows covered entities to disclose protected health information to these business associates if the covered entities obtain satisfactory assurances, or business associate agreements, that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under HIPPA.

(ix.) The disclosure is to the DOA Bureau of Audits to facilitate the provision of audit services.

(x.) The disclosure is to the DOA Division of Information Technology in order to perform technological services including the maintenance of information technology security.

(xi.) The disclosure is to the DOA Division of Legal Services to facilitate the provision of legal services.

(xii.) The disclosure is to DOA's Privacy Officer for investigation of a HIPAA complaint or as otherwise directed by him/her. Currently, Michael Sligar, Esq. is DOA's designated Privacy Officer. He may be reached at 574-8535 or Michael.sligar@doa.ri.gov.

(xiii.) The disclosure is authorized in writing by the Privacy Office and is:

1. Required by law.

2. For public health activities.

3. Related to a victim of abuse, neglect or domestic violence.

4. Related to health oversight activities.

5. Made in response to an order from a judicial or administrative proceeding.

6. Made for law enforcement purposes.

7. Related to a decedent.

8. Related to cadaveric organ, eye or tissue donation purposes.

9. Related to research purposes.

10. Related to the aversion of a serious threat to health and safety.

11. Related to a specialized government function.

b. Employees may, but are not required to, disclose limited relevant PHI to a family member or friend who has been specifically identified by the participant or who is directly involved in the care of the participant, or the payment for care. Disclosure should only occur after verification of identity and authority, and should utilize the minimum necessary rule defined herein.

c. Whenever an employee makes an allowable disclosure of a participant's PHI, they shall make note of the event in a PHI disclosure log. The notation shall include the date of the disclosure, the PHI disclosed, the name of the person to whom the disclosure was made, and the justification for the disclosure.

d. Whenever an employee is unsure of the propriety of a disclosure, he/she shall err on the side of caution and first contact the Privacy Officer for discussion and guidance.

4. II. Minimum Necessary Rule

a. When a disclosure of Pill is permitted, employees of DOA health care components shall disclose only the amount of PHI that is the minimum necessary to accomplish the intended purpose.

b. The minimum necessary rule does not apply to the following:

(i.) Disclosures to a health care provider for treatment purposes.

(ii.) Disclosures to the individual who is the subject of the information.

(iii.) Disclosures authorized by the individual pursuant to a HIPAA-compliant authorization, in a form provided by the Privacy Officer.

(iv.) Disclosures required for compliance with HIPAA.

(v.) Disclosures to the federal Department of Health and Human Services when disclosure of information is required under HIPAA for enforcement purposes.

(vi.) Disclosures that are required by other law.

5. Participants' Core HIPPA Rights

a. Employees shall always respect participants' core HIPPA rights:

(i.) To receive a copy of the DOA Notice of Privacy Practices.[3]

(ii.) To request restrictions and confidential communications of his/her PHI.

(iii.) To inspect and/or receive an electronic copy of his/her healthcare records.

(iv.) To request corrections of his/her healthcare records.

(v.) To obtain an accounting of disclosures (i.e., a list showing when and with whom his/her PHI has been shared).

(vi.) To file a complaint with DOA and the federal government if the individual believes his/her rights have been denied or that his/her PHI is not being protected.

(vii.) To receive a notice of a breach of his/her unsecured PHI.

b. Employees shall never intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual who exercises any core HIPAA right.

6. Employee Administrative, Physical and Technological Safeguard Obligations

a. All employees shall ensure the confidentiality and security of PHI by observing the following practices:

(i.) Never allow unauthorized persons access to computers or workspaces.

(ii.) Keep computer passwords secret; never write passwords on sticky notes left on a computer, never share passwords with other staff members, and never use the same password for everything.

(iii.) Use password-protected screensavers for added privacy.

(iv.) Place a computer screen so that it cannot be viewed by unauthorized individuals.

(v.) Keep notes and files in a secure place; never leave them in open areas outside workspaces.

[3] The DOA Notice of Privacy Practices shall be available on the OEB website (www.employeebenefits.ri.gov), shall be mailed to a participant upon request and without charge, and shall be available in hard copy from OEB or from the Privacy Officer.

(vi.) Make certain when mailing documents that no sensitive information is shown on postcards or through envelope windows, and that envelopes are closed securely.

(vii.) When disposing of sensitive information, personally shred documents or use locked shredding drop boxes.

(viii.) Use caution and discretion when conducting conversations in DOA office spaces such that PHI is not inadvertently disclosed.

(ix.) Encrypt emails when PHI needs to be included.

1. To encrypt an email, type [encrypt], [send secure] or <send secure> in the Subject field of the message. Make sure to include the square brackets or the greater than and less than symbols.

(x.) Unless absolutely necessary as determined and approved by the Privacy Officer, never place PHI on a mobile device.

1. If PHI must be placed on a mobile device, only use devices approved by the Division of Information Technology.

7. Breach

a. All employees shall promptly report to the Privacy Officer any incidents involving improper disclosures or possible breaches. A breach is, generally, an impermissible use or disclosure under HIPAA that compromises the security or privacy of the PHI.[4] In the event of a breach, the DOA HIPAAI/HITECH Breach Notification Policy (DOA-HIPAA-3) provides procedures for response and notification.

8. Sanctions

a. DOA shall apply appropriate sanctions against employees who fail to comply with the HIPAA Confidentiality Policy and its underlying procedures. Levy of sanctions is at the discretion of the DOA Director.

9. Signatures

Director of Administration

[4] An impermissible use or disclosure of PHI is presumed to be a breach unless DOA can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHJ or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.