State of Rhode Island
Department of Administration
Policies and Procedures
Department of Administration's Designation as a Hybrid Entity under HIPAA

Approved By:	**Policy Number: DOA-HIPAA-1**
Date Approved:	**Date Policy Last Revised: 9/26/18**

HYBRID ENTITY DESIGNATION

The Department of Administration ("DOA") has determined that it meets the criteria of a hybrid entity under the Health Insurance Portability and Accountability Act of 1996, and the regulations promulgated thereunder ("HIPAA"). This determination was made after an analysis of the law and regulations in relationship to various divisions and offices within DOA. As a hybrid entity, DOA is a single legal entity[1] whose business activities include both covered and non-covered functions under HIPAA.[2] While the primary purpose of DOA is not to be a health care provider, health care plan, or health care clearinghouse, some of DOA's components perform covered functions. Components that perform covered functions are "health care components" and are subject to HIPAA, while the remainder of DOA is not.[3] By designating certain divisions and offices as HIPAA-covered health care components, DOA limits its HIPAA compliance obligations to those units.[4]

DOA's HIPAA-covered health care components are:

1. **Office of Employee Benefits** ("OEB")
    a. OEB administers the State's employee health care plan (medical, vision and dental), medical flexible spending plan, and wellness program.
    b. If it were a separate legal entity, OEB would be a covered entity under HIPAA.[5]
2. **Division of Legal Services ("Legal Services") and Bureau of Audits ("Audits")**:
    a. Legal Services and Audits access Protected Health Information (including electronic Protected Health Information, together "PHI"),[6] acquired and maintained by OEB, and are designated as health care components only to the extent they receive, maintain, or transmit PHI as follows:[7]
        i. Legal Services is designated as a DOA health care component only to the extent that any PHI is disclosed in the course of providing legal advice and legal services to OEB.
        ii. Audits is designated as a DOA health care component only to the extent that any PHI is disclosed in the course of providing audit services to OEB or to the Executive Office of Health and Human Services as part of its function as a Medicaid provider.

---

[1] Pursuant to R.I. Gen. Laws §§ 42-6-1 and 42-11-1, DOA is established as a department within the executive branch of the state government.
[2] 45 C.F.R. §164.103. "Covered functions" are "those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse."
[3] 45 C.F.R. §164.105.
[4] 45 C.F.R. §164.105(a)(1)
[5] 45 C.F.R. §160.103.
[6] *Id.*
[7] 45 C.F.R. §164.105 (a)(2)(i)(C) & (D).

This list could change in the future if certain business practices change. Until that time, only the above-listed DOA health care components are required to comply with HIPAA.

SAFEGUARD REQUIREMENTS

As a hybrid entity, DOA must ensure that a health care covered component complies with applicable HIPAA requirements[8] including, but not limited to, the following:

1. The release of PHI from a DOA health care component to a DOA non-health care component is considered a disclosure under HIPAA and is not permitted unless there is an individual authorization or a specific exemption allowing the disclosure.
2. HIPAA's Privacy Rule[9] requires DOA to implement protections between the health care and non-health care components to assure that PHI is not improperly disclosed.
3. If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose PHI created or received in the course of, or incident to, the member's work for the health care component.

RETENTION

Designation of health care components shall be maintained for at least six-years following termination of any division or department as a health care component and indefinitely for existing health care components.[10]

POLICY

This policy is effective upon approval and shall supersede all previously issued policies. This policy may be amended or revoked at any time without notice.

NONCOMPLIANCE

Any entity or person who violates this policy may be subject to disciplinary action up to and including termination.

QUESTIONS

Please refer to the DOA HIPAA Privacy and Security Policy and Procedures document, DOA-HIPAA-2. Contact the DOA HIPAA Privacy Officer Jennifer S. Sternick, Esq. at (401) 222-8880. Contact the DOA HIPAA Security Officer Brian Tardiff at (401) 462-1783.

APPROVAL

Michael DiBiase, Director, Department of Administration

[8] 45 C.F.R. §164.105(a)(ii) & (iii).
[9] 45 C.F.R. §164.500 *et seq.*
[10] 45 C.F.R. §164.105(c)(2).

State of Rhode Island
Department of Administration
Policies and Procedures
HIPAA Confidentiality

Policy Number: DOA-HIPAA-2	Date Policy Last Revised: 9/8/16

POLICY

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) ("HIPAA") and must provide confidentiality protections for any individually identifiable health information ("PHI" or "protected health information") it maintains or has access to.

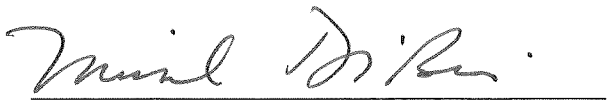
DOA has designated itself as a "Hybrid Entity" in accordance with HIPAA. See Department of Administration's Designation as a Hybrid Entity under HIPAA, DOA-HIPAA-1. The health care components of DOA shall operate in conformance with the administrative, physical and technological requirements of HIPAA, 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]

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.

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.

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

APPROVAL



Michael DiBiase, Director, Department of Administration

[1] Modifications to the HIPAA 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 HIPAA Rules; Final Rule, 78 Fed. Reg. 5565 (Jan. 25, 2013) (amending 45 C.F.R. Parts 160 and 164). Available at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

PROCEDURES

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 TPA maintains detailed records with respect to a participant's visits to medical providers and the claims and payments arising from those 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.

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.

I. Disclosures of PHI

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]

[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 HIPAA.

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.
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.
xiii. The disclosure is authorized in writing by the Privacy Officer and is:
    a) Required by law.
    b) For public health activities.
    c) Related to a victim of abuse, neglect or domestic violence.
    d) Related to health oversight activities.
    e) Made in response to an order from a judicial or administrative proceeding.
    f) Made for law enforcement purposes.
    g) Related to a decedent.
    h) Related to cadaveric organ, eye or tissue donation purposes.
    i) Related to research purposes.
    j) Related to the aversion of a serious threat to health and safety.
    k) Related to a specialized government function.

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.

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.

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.

II. Minimum Necessary Rule

When a disclosure of PHI 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.

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.

III. Participants' Core HIPAA Rights

Employees shall always respect participants' core HIPAA 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.

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

IV. Employee Administrative, Physical and Technological Safeguard Obligations

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.
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.

[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 form OEB or from the Privacy Officer.

ix. Encrypt emails when PHI needs to be included.
   a. 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.
   a. If PHI must be placed on a mobile device, only use devices approved by the Division of Information Technology.

V. Breach

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 HIPAA/HITECH Breach Notification Policy (DOA-HIPAA-3) provides procedures for response and notification.

VI. Sanctions

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.

---

[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 PHI 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.

State of Rhode Island
Department of Administration
Policies and Procedures
Department of Administration's HIPAA/HITECH Breach Notification Policy

Policy Number: DOA-HIPAA-3	Date Policy Last Revised: 9/8/16

POLICY

In the event of a breach in acquisition, access, use, or disclosure of Unsecured Protected Health Information, in a manner not permitted under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which compromises the security or privacy of the Unsecured Protected Health Information, the health care components of the Department of Administration ("DOA") shall operate in conformance with the requirements of HIPAA, 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]

The DOA HIPAA Privacy and Security Officers are authorized to promulgate new procedures and amend existing procedures to effectuate DOA's conformance with the breach notification provisions of HIPAA, GINA, HITECH and the regulations promulgated thereunder, including, but not limited to, the Omnibus Rule.

APPROVAL

Michael DiBiase, Director, Department of Administration

PROCEDURES

[1] Modifications to the HIPAA 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 HIPAA Rules; Final Rule, 78 Fed. Reg. 5565 (Jan. 25, 2013) (amending 45 C.F.R. Parts 160 and 164). Available at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

Section 1. Definitions

a. **Breach:** Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA, which compromises the security or privacy of the protected health information. The security or privacy of PHI is compromised when there is a significant risk of financial, reputational or other harm to the affected individual. Breach excludes:

   i. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA.

   ii. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.

   iii. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

b. **DOA:** DOA means the health care components of DOA, as indicated in DOA's "Designation as a Hybrid Entity under HIPAA" (DOA-HIPAA-1).

c. **Protected Health Information (PHI):** PHI means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

d. **Unsecured Protected Health Information (Unsecured PHI):** Unsecured PHI means any PHI which is not unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology, such as encryption or destruction, as specified by the Secretary of DHHS.

e. **Workforce:** Workforce means employees, volunteers, trainees, and other persons under the direct control of DOA Health Care Components, whether or not they are paid by DOA.

Section 2. Breach

In summary, HIPAA requires that covered entities notify individuals whose Unsecured PHI has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the PHI. The notification requirements only apply to breaches of Unsecured PHI. In other words, if PHI is encrypted or destroyed in accordance with the HIPAA guidance, there is a "safe harbor" and notification is not required.

2.1 Discovery of Breach.

A breach shall be treated as discovered as of the first day on which such breach is known to DOA or, by exercising reasonable diligence, would have been known to DOA or any person, other than the person committing the breach, who is a workforce member or agent of DOA.

Workforce members who believe that unsecured PHI has been used or disclosed in any way that compromises the security or privacy of that information shall immediately notify their supervisor(s), the DOA Division of Legal Services (222-8880), and the DOA Privacy and Security Officers.[2]

Following the discovery of a potential breach, DOA shall begin an investigation, conduct a risk assessment, and, based on the results of the risk assessment, begin the process of notifying each individual whose PHI has been, or is reasonably believed by DOA to have been accessed, acquired, used, or disclosed as a result of the breach. DOA shall also begin the process of determining what notifications are required or should be made, if any, to the DHHS Secretary, media outlets, or law enforcement officials.

2.2 Breach Investigation.

DOA's Privacy and Security Officers shall act as joint investigators of the breach. The investigators shall be responsible for the management of the breach investigation, completion of the risk assessment, and coordinating with others in DOA as appropriate. DOA's entire workforce is expected to assist management in this investigation as requested. The investigators shall be the key facilitators for all breach notification processes.

2.3 Risk Assessment.

For breach response and notification purposes, a breach is presumed to have occurred unless DOA can demonstrate that there is a low probability that the PHI has been compromised based on, at minimum, the following risk factors:

2.3.1 The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

---

[2] Currently, the DOA HIPAA Privacy Officer is Jennifer S. Sternick, Esq. in the Division of Legal Services. She can be reached by phone at 222-8880 and by email at jennifer.sternick@doa.ri.gov. The DOA HIPAA Security Officer is currently Kurt Huhn in the Division of Information Technology. He can be reached by phone at 462-706 and by email at kurt.huhn@doit.ri.gov.

2.3.2 The unauthorized person who used the PHI or to whom the disclosure was made.

2.3.3 Whether the PHI was actually acquired or viewed.

2.3.4 The extent to which the risk to the PHI has been mitigated.

The evaluation should consider these factors, or more, in combination to determine the overall probability that PHI has been compromised. The risk assessment should be thorough and completed in good faith, and the conclusions should be reasonable.

Based on the outcome of the risk assessment, DOA will determine the need to move forward with breach notification. The investigators must document the risk assessment and the outcome of the risk assessment process. All documentation related to the breach investigation, including the risk assessment, must be retained for a minimum of six years.

2.4 Notification: Individuals Affected.

If it is determined that breach notification must be sent to affected individuals, DOA shall attempt to notify all affected individuals. DOA also has the discretion to provide notification following an impermissible use or disclosure of PHI without performing a risk assessment, if DOA so chooses. Written notice to affected individuals shall be written in plain language and must contain the following information, which elements are included in DOA's standard breach notification letter:

2.4.1 A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

2.4.2 A description of the types of Unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).

2.4.3 Any steps the individuals should take to protect themselves from potential harm resulting from the breach.

2.4.4 A brief description of what DOA is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

2.4.5 Contact procedures for individuals to ask questions or learn additional information.

Written notification will be sent by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If DOA knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written

notification by first-class mail to the next of kin or personal representative shall be carried out.

If there is insufficient or out-of-date contact information that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. If there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, by telephone, or by other means. If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of DOA's website, or a conspicuous notice in major print or broadcast media in DOA's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

Notice to affected individuals shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. If DOA determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate, in addition to the methods noted above. It is the responsibility of DOA to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

2.5 Notification: DHHS.

In the event a breach of unsecured PHI affects 500 or more individuals, DHHS will be notified at the same time notice is made to the affected individuals, in the matter specified on the DHHS website.[3] If fewer than 500 individuals are affected, DOA will maintain a log of the breaches to be submitted annually to the DHHS Secretary no later than 60 days after the end of each calendar year, in the manner specified on the DHHS website.[4] The submission shall include all breaches discovered during the preceding calendar year.

2.6 Notification: Media.

In the event the breach affects more than 500 residents of a state, prominent media outlets serving the state and regional area will be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a press release.

2.7 Delay of Notification Authorized for Law Enforcement Purposes.

---

[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html
[4] Id.

If a law enforcement official states to DOA or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, DOA shall:

2.7.1 If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

2.7.2 If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

This applies to notices made to individuals, the media, DHHS, and by business associates.

2.8 Maintenance of Breach Information.

DOA shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of individuals affected. The following information should be collected for each breach:

2.8.1 A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known.

2.8.2 A description of the types of unsecured PHI that were involved in the breach.

2.8.3 A description of the action taken with regard to notification of individuals regarding the breach.

2.8.4 Steps taken to mitigate the breach and prevent future occurrences.

DOA shall maintain each log of breach-related information for no less than five years.

2.9 Business Associate Responsibilities.

DOA's business associates shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach of unsecured PHI, notify DOA of such breach. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. The business associate shall provide DOA with any other available information that DOA is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the business associate of discovery of a breach, DOA will be responsible for notifying affected individuals, unless otherwise agreed upon by the business associate to notify the affected individuals.

2.10 Complaints.

DOA provides a process for individuals to make complaints concerning DOA's HIPAA privacy and security policies and procedures or its compliance with such policies and procedures. Individuals also have the right to complain about DOA's breach notification processes.

2.11 Sanctions.

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

2.12 Retaliation/Waiver.

DOA may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his/her privacy rights. Individuals shall not be required to waive their privacy rights as a condition of enrollment in the State employee health plan or eligibility for benefits.