

**Compliance and Clinical Affairs Office
Policies and Procedures**

Subject: Incident Response Plan	Policy #: BREACH 01
Effective date: July, 2013	Pages: 6
Additional Areas of Impact: Puerto Rico Health Insurance Administration and its contractors	
Reference: Section 13402 of Health Information Technology for Economic and Clinical Health Act (HITECH), Health Insurance Portability and Accountability Act of 1996 (HIPAA) and part of American Recovery and Reinvestment Act 2009 (ARRA), BCBSA HIPAA Privacy and Security Requirements Category 5 Regulatory MA 5.03 Breach and Security Incident Handling, 42 CFR § 160.400 Section of HIPAA Privacy Policy, 45 C.F.R. sec. 164.404 and 45 C.F.R. sec. 406	

Policy Statement:

HIPAA covered entities and their business associates are required to provide notification following a breach of unsecured protected health information as required by the interim final breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Objective:

The objective of this policy is to establish guidance and procedure when an incident occurs. The Incident Response Plan will include actions to be followed when a breach of unsecured information, any potential threat to computers/data, or any source of the intrusion or incident at a third party is traced back to the organization.

Purpose:

The key principles of incorporating this Incident Response Policy are listed below:

- To implement a protocol plan that meets with both HIPAA and HITECH requirements.
- To provide an approved timeframes to report any identified breach to individuals, government agencies and business associate.
- To designate an incident response team and roles.

Definitions:

1. **Security Breach** - is defined as unauthorized acquisition of data that compromises the security, confidentiality or integrity of personal information maintained by us. Good faith acquisition of personal information by an employee or agent of our company for business purposes is **not** a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

2. **Personally Identifiable Information (PII)** - is defined as an individual's first name or first initial and last name, in combination with any of the following data: Social Security number; driver's license number or identification card number, financial account number, credit or debit card number, number such as an access code, security codes or password that would permit access to an individual's financial account, home address or e-mail address and medical or health information.

3. **Protected Health Information (PHI)**- is the individually identifiable health information held or transmitted in any form or medium by these HIPAA covered entities and business associates, subject to certain limited exceptions.

4. **Business Associate** - means a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of individually identifiable health information.

5. **Covered entity**- is a health plan, health care clearinghouse, or health care provider that transmits any health information electronically in connection with a covered transaction, such as submitting health care claims to a health plan.

Responsibilities:

Puerto Rico Health Insurance Administration (ASES) is responsible for establishing and implementing policies and procedures to conduct risk assessments, assess privacy or security breach incidents, provide affected individuals required notifications and report government agencies of incident in a timely manner, in compliance with regulation and legal statutes.

Policy:

The Incident Response Plan (IRP) is implemented to handle any privacy or security situation in a way that limits any possible impact to PHI and PII. This IRP is a guideline that delineates actions to be taken when an incident or breach occurs.

Breaches Notification Requirements

The Incident Response Team will coordinate notifications to affected individuals, business associates, as well as to the corresponding regulatory agencies within the timeframes established by regulation as seen below:

- **Individual Notice** - ASES must notify affected individuals following the discovery of a breach of unsecured protected health information and must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the affected individual exceeds 10 or more, ASES entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If ASES has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Please refer to the *HIPAA Breach Notification Model Letter*.

- **Notification to Government Agencies** - must notify the Secretary of breaches of unsecured protected health information. ASES and the MCO will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, must notify the Secretary without unreasonable delay and in no case later than 60 calendar days following a breach. If, however, a breach affects fewer than 500 individuals, ASES may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred. For both under or over 500 individuals affected there are instructions for submitting the notice to the Secretary. The organization will provide a report to DACO within fourteen (14) days of the discovering of the Breach.
- **Notification to Business Associate** - If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify ASES following the discovery of the breach. A business associate must provide notice to ASES without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide ASES with the identification of each individual affected by the breach as any information required to be provided by ASES in its notification to affected individuals

Elements for Notification to the Media:

For a breach that affects more than 500 individuals, ASES and the MCO must include in the media notification the following elements:

- 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) A description of the types of unsecured protected health information 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);
- 3) Any steps individuals should take to protect themselves from potential harm resulting from the breach

4) A brief description of what the ASES involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Incident Response Team:

In the event that a breach occurs, it should be reported immediately upon discovery to the Incident Response Team. The Incident Response Team is a group of people authorized to take appropriate steps deemed necessary to contain, mitigate, resolve, and report a privacy or security incident. This team will be responsible of determining the root cause of the situation and its scope, containing the problem, and investigating the origin of the incident in order to prevent the possibility of recurrence. Please refer to the *Attachment A*

Roles and Duties:

Compliance Department:

- Detection of a Privacy Breach
- Communication of breach to the Chief Compliance and Privacy Officer and Senior Management
- Defining the incident by identifying what happened, when and where, and who was involved in it
- Performing an assessment of the breach and its possible impact
- Keeping inventory of confidential materials at risk
- Containing the incident's damage such as taking steps to prevent further unauthorized access (example: stop a mailing)
- Detailed documentation of the incident in a predefined protocol (Privacy/Security Breach Internal Report)
- Providing notification of privacy or security breach to affected plan members in accordance to regulations and timeframes
- Reporting to external regulatory agencies (example: CMS, HHS, PRHIA) in accordance to regulations and timeframes
- All incidents must be recorded in a Master Log including the preliminary details of the breach, when, how, who, or what was affected
- Establishing recommendations for corrective actions and guidelines that increase privacy and security and reduce vulnerability to any comparable incident
- Monitoring and testing established privacy controls and documenting findings or outcomes
- Assess the need to change privacy policies, procedures and/or practices as a result of the breach.

Information Technology Department:

- Detection of a Security Breach (central point of contact for all computer incidents)
- Communication of breach to the Chief Information and Security Officer and Senior Management
- Defining the incident by identifying what happened, when and where, and who was involved in it
- Determining which electronic PHI (ePHI) and other sensitive information has been affected.
- Performing an assessment of the breach and its possible impact
- Search for any signal of a firewall breach
- Identifying security measures that were circumvented
- Containing the incident's damage such as taking steps to prevent further unauthorized access (example: password change)
- Assess the likelihood of recovering
- Determining if lost data can be restored from backups and if lost data can be neutralized by changing account access, ID information, and others.
- Detailed documentation of the incident in a predefined protocol (Privacy/Security Breach Internal Report)
- Monitoring and testing systems to ensure compliance with the information security rule and controls and documenting findings or outcomes
- Document and provide the Compliance Department a complete assessment and report of the breach

Law enforcement delay

ASES may delay notifications processes due to criminal investigations or cause damage with the national security requested by law enforcement official. Requests can be orally or in a written form. If the delay request has been orally, ASES' employee must document the request, including the identity of the official making the request, and delay the notification, notice or posting temporarily and no longer than 30 days from the date of the oral request. If delay' request in written and specifies the time for which such delay is required ASES will delay for no longer than 30 days of the notification letter' date.

After a Breach.

After a privacy or security breach, Puerto Rico Health Insurance Administration, must:

- Evaluate the incident with respect to the organization Privacy and Security Compliance requirements
- Provide guidance or retraining of policies and procedures to prevent the incident from occurring again
- Revise or develop new policies and procedures
- Develop and implement additional safeguards to protect PHI/PII
- Monitoring and testing privacy and security practices.

Document Retention

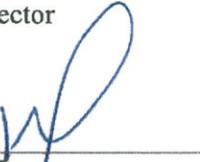
All the documents related to breaches will be preserved for a minimum period of ten (10) years.

Revised By: 
Privacy Officer

Date; _____

Revised and Approved By: _____
Legal Department Director

Date; _____

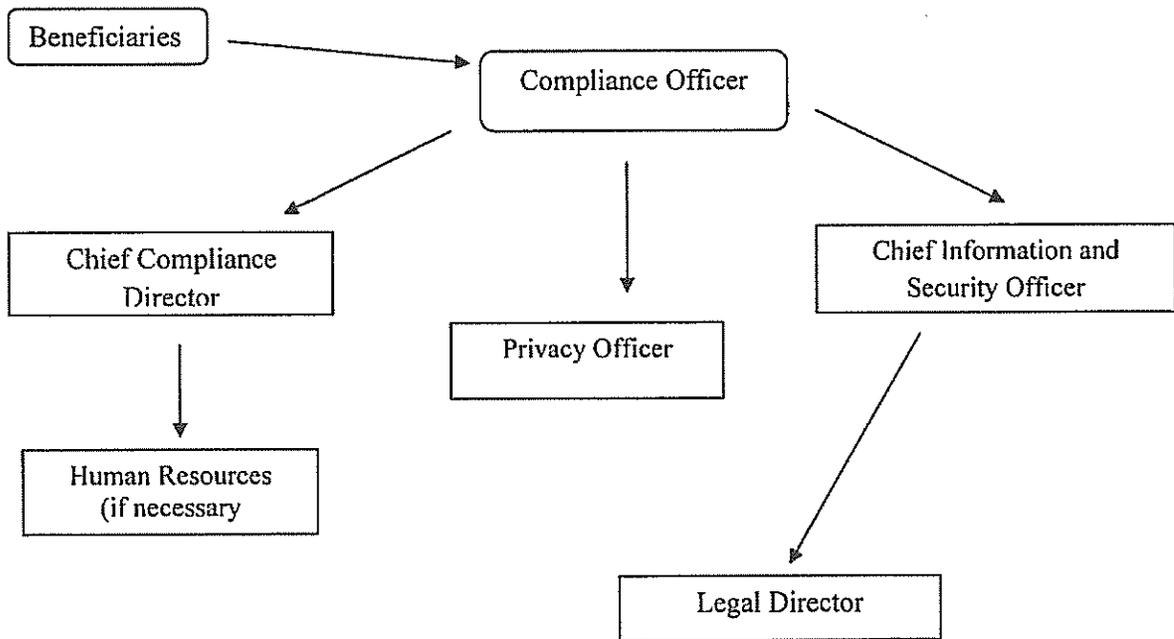
Approved By: 
Chief Compliance Officer

Date: _____

Attachment A

Incident Response Team

The Incident Response Team is composed of personnel from the Compliance Department and Information Technology Department, depending on the type of breach, (Privacy or Security) supported and guided by the *Chief Compliance Director*, *Privacy Officer* and the *Chief Information and Security Officer*.



****Currently under review****