Americare Certified Special Services
Policy, Procedures and Information

Title: Breach Notification Policy	**Effective Date: 9/23/13**
	Last Revision: N/A
Issued By: Miri, Bank RN - Director of Compliance	**Approved by: Professional Advisory Committee**
	REFERENCE: 45 CFR Part 164

PURPOSE: To establish a process for notifying patients of a Breach of their Unsecured Protected Health Information ("PHI") in conformance with the requirements imposed under the Health Insurance Portability and Accountability Act (HIPAA) and the regulations promulgated thereunder and the Secretary of Health and Human Services, as applicable.

POLICY: Americare Specialty Services, Inc., ("Americare") has implemented reasonable and appropriate Administrative, Physical and Technical Safeguards to protect the confidentiality, integrity and availability of PHI in its possession. Americare has implemented reasonable systems for the discovery and reporting of a Breach of PHI.

DEFINITIONS:

1. **Breach of PHI:** The acquisition, access, use or disclosure of PHI in a manner not permitted under the Health Insurance Portability and Accountability Act ("HIPAA") regulations which compromises the security or privacy of the PHI. All unauthorized acquisitions, access, uses, or disclosures of Unsecured PHI will require a risk assessment to determine whether a Breach has occurred.

Exceptions: A Breach shall not include:

a. Any unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of Americare or a Business Associate of Americare, 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 prohibited under HIPAA.

b. Any inadvertent disclosure by a person who is authorized to access Protected Health Information at Americare or at one of Americare's Business Associates to another person authorized to access the Protected Health Information at Americare or one of its business associates, or organized health care arrangement in which Americare

participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.

c. A Disclosure of Protected Health Information where a Americare or an Americare 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.

2. **Business Associate:** A person or entity who performs functions or activities on behalf of, or certain services for, Americare that involve the use or disclosure of PHI. Business Associates of Americare are required to immediately report all breaches, losses, or compromises of PHI – whether secured or unsecured – to Americare's Chief Compliance Officer.

3. **Disclosure:** The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

4. **Protected Health Information or PHI:** Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Individual identifiable health information is information that is a subject of health information, including demographic information collected from an individual, and:

a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse, and

b. Relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

i. That identifies the individual; or

ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

5. **Unsecured PHI:** Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services. At this time, destruction and encryption are the only approved technology or methodology. HHS Guidance:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

PROCEDURE:

Whenever a member of the Americare workforce or a Business Associate suspects that there has been an unauthorized acquisition, use or disclosure of PHI they shall immediately notify the Director of Compliance. Director of Compliance shall undertake an investigation to determine whether a Breach has occurred.

A. STEP ONE: Determine Whether the PHI was unsecured: The Compliance Officer shall determine whether the information was unsecured PHI. If it is determined that the information was not Unsecured PHI, no further action is necessary.

B. STEP TWO: Determine Whether a Breach Exception Applies. The Compliance Officer needs to determine whether an exception to the definition of a breach applies. If an exception applies not further action is required.

C. STEP THREE: **Conduct a Risk Analysis.** If it is determined that the PHI was unsecured and no exception applies, the Compliance Officer shall conduct a risk analysis that considers at least the four factors listed below to determine whether a Breach has occurred. In accordance with HIPAA regulations, it is presumed that the unauthorized use or disclosure is a Breach unless it can be demonstrated that there is a <u>low</u> probability that the PHI has been compromised.

i. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
ii. the unauthorized person who used the PHI or to whom the disclosure was made;
iii. whether the PHI was actually acquired or viewed; and
iv. the extent to which the risk to the PHI has been mitigated.

If the information disclosed constitutes Unsecured PHI and the Director of Compliance determines that the disclosure of such information constitutes a Breach, the Director of Compliance shall, to the extent practicable, seek to mitigate any harm caused by the Breach and provide all notices required under this policy.

STEP FOUR: NOTIFICATIONS, IF REQUIRED

<u>Notice to Individuals Impacted by Breach</u>:

Notice will be provided to affected individuals by the HIPAA Security Officer as soon as possible and in no case later than sixty (60) days after discovery of the Breach.

The notice shall be sent by first class mail or if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail, and shall be written in plain language.
If Americare knows the patient is deceased and has an address of next of kin or a personal representative, the notice will be sent by first class mail to the next of kin or personal representative.
In cases where insufficient or out-of-date contact information exists, Americare shall use substitute means for notice.

If at any time the Breach is deemed to require urgent notice due to the risk of possible imminent misuse of unsecured PHI, Americare shall provide notice to patients by telephone or other means in addition to the notice provided by first class mail.

Exception: If Americare receives a request by a law enforcement officer to delay notice because the provision of such notice would impede a criminal investigation or cause damage to national security, Americare shall:

1. If the statement is in writing, delay the notice or posting for the time period specified in the notice; or

2. If the statement is made orally or the writing does not provide a time period for delay, delay the notice or posting for no more than thirty (30) days. If the request is made orally, Americare shall document the request including the identity of the individual making the request.

Contents of Patient Notice: In all cases the notice must contain the following information:

1. A brief description of what happened, including the date of the Breach and date of discovery of the Breach;

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);

3. Any steps individuals should take to protect themselves from potential harm resulting from the Breach;

4. A brief description of the investigation into the Breach, mitigation harm to individuals, and protection against any further breaches; and

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

6. Any additional information required by applicable state privacy or consumer protection law.

Notice to the Media: When a Breach is discovered that involves Unsecured PHI for more than 500 individuals Americare shall notify prominent media outlets.

Notice to Secretary of HHS: Americare shall notify the Secretary of HHS of Breaches of Unsecured PHI.

1. ***500 or More*:** In the case of Breaches involving 500 or more individuals, Americare shall provide notice to the Secretary contemporaneously with the notice provided to patients and in the manner specified on the HHS website:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

2. ***Less than 500*****:** In the case of breaches involving fewer than 500 individuals Americare shall maintain a log of all breaches. The log shall contain:

a. The number of individuals affected by the Breach;

b. The type of Breach (e.g., theft, loss, improper disposal, unauthorized access, hacking or other IT incident);

c. The location of the Breach (e.g., laptop, desktop computer, network server, e-mail, other portable electronic device, electronic medical record, paper record, etc.);

d. The type of PHI involved in the Breach (e.g., demographic, financial, or clinical);

e. A brief description of the Breach including the location of the Breach, how the Breach occurred, the type of Breach, the media involved, and the type of PHI involved in the Breach;

f. The safe guards that existed prior to the Breach (e.g., firewalls, packet filtering, secure browser sessions, strong authentication, encrypted wireless, physical security, logical access control, anti-virus software, intrusion detection, biometrics);

g. Information regarding the notice provided (i.e., date of notice, whether substitute notice was required, and whether media notice was provided); and

h. Description of actions taken in response to the Breach.

No later than sixty (60) days after the end of each calendar year, Americare shall notify the Secretary of HHS regarding the Breaches involving less than 500 individuals discovered during the preceding calendar year. The notice shall be made in the manner specified on the HHS website:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Training: The **HIPPA Privacy Officer** or her designee shall implement an initial and annual training program on this policy and the Breach Notification Rule for all existing and newly employed workforce members of Americare.