Reporting A Privacy And Or Security Breach

Purpose
This procedure establishes the required reporting of alleged or actual privacy and/or security breaches. As a contracted Business Associate of covered entities, we are required to report breaches of unsecured protected health information in accordance with privacy and security regulations. Additionally, many states have data breach notification laws that require covered entities to report incidents and notify affected individuals.

Scope
The scope of this procedure is applicable for all incidents of alleged or actual privacy and / or security breaches.

Definitions
Protected Health Information *as defined by the federal privacy regulation is information that:*

- *Contains data elements or combinations of data elements that could identify a person, or provides a reasonable basis to believe someone could be identified;*
- *Contains health-related information about that person; and*
- *Is maintained or transmitted in any form (electronic, written, or oral)*

Breach – *the unintentional or unauthorized release of Protected Health Information.*

Policy
Our agency requires all associates and subcontractors to report any suspected breach of protected health information in accordance with legal and contractual requirements. Any and all suspected breaches of protected health information will be reported immediately to our designated Privacy & Security Official for investigation.

The Privacy & Security Official will quickly analyze the report of suspected or actual breach information to assess for potential risks and to determine whether a breach of unsecured protected health information has occurred. The assessment will also include a review on the level of risk and potential harm to the individual(s).

Our Privacy & Security Official will notify the Privacy Office of the covered entity of any incident without unreasonable delay and in any event no later than timeframe documented in the business associate agreement.

Our Privacy & Security Official and the designated contact from the covered entity Privacy Office will jointly discuss and determine notification requirements to be compliant with state and federal laws.

Procedure
1. An actual or suspected breach of protected health information should be reported to the Privacy & Security Official as quickly as situation is determined.
2. Provide all information regarding the suspected incident to the Privacy & Security Official or complete an incident notification form if available. At a minimum the information provided should include: names, dates, nature of the protected health information, the manner of the unauthorized use or disclosure and any written or electronic documentation concerning the incident.
3. Upon receipt of potential breach incident, the Privacy & Security Official will promptly conduct an investigation and assess risk of incident.
4. Privacy & Security Official will review contractual agreements with impacted covered entities to obtain reporting information, process and contact.
5. The Privacy & Security Official will report the privacy incident to the covered entity's Privacy office as quickly as discovery of the breach but not later than timeframes indicated within covered entity Business Associate agreement.
6. The Privacy & Security Official will provide the covered entity the following information regarding the suspected / alleged privacy and/or security breach: identification of each individual whose unsecured protected health information has alleged to have been accessed, acquired or disclosed, a description of the event, date of potential breach, type of protected health information involved

in incident, any preliminary steps that have been taken to mitigate the damage and description of investigatory steps taken to date or complete an incident notification form provided by a covered entity.

7. The Privacy & Security Official will cooperate and assist the covered entity's Privacy Office with mitigation of risk of harm, required notifications, implementation of any corrective actions, & retraining of associates. Review of the executed Business Associate Agreement will also assist with responsibilities and obligations regarding notification methods and contents.
8. The Privacy & Security Official will document all actions of every incident in detail and retain documentation for a period of at least six years or follow agency retention requirements.

ADOPT

Return / Destruction of Protected Health Information upon Contract Termination

Purpose

This procedure is to provide guidelines on the required return or destruction of protected health information upon termination of contract with a covered entity in accordance with contractual agreements.

Scope

The scope of this procedure is applicable for our agency and any subcontractors having access to protected health information of our covered entity(ies).

Definitions

Protected Health Information as defined by the federal privacy regulation is information that:

- Contains data elements or combinations of data elements that could identify a person, or provides a reasonable basis to believe someone could be identified;
- Contains health-related information about that person; and
- Is maintained or transmitted in any form (electronic, written, or oral)

Policy

In accordance with the requirements of our executed Business Associate Agreements with covered entities, our agency is required to return or destroy protected health information of the covered entity upon contract termination. Our agency will contact the covered entity to discuss the best method of returning or destroying protected health information that was received, created or retrieved by our agency on behalf of the covered entity.

In the event that immediate contact can't be made, our agency will continue to protect and safeguard the protected health information and limit further use or disclosure of such information until return / destruction has occurred.

Procedure

1. Upon notification or decision that contract between our agency and covered entity has been terminated or will be terminated, agency Privacy and Security Official shall contact the covered entity to discuss most appropriate method for return or destruction of protected health information.
2. Privacy Official will follow directions provided by the covered entity regarding the return or destruction of data and verify that all actions are complete.
3. Privacy Official will document completed actions.