Security Policies and Procedures

**Policy Title:** Security Breach Notification

Policy Number: Effective Date:

Date Last Revised: Revision Number:

Approved/Reviewed by:

**Policy: Company will comply with all federal and state laws and regulations requiring the notification of privacy and security breaches.**

**Definitions:**

**Breach** means generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

This includes when PHI has potentially been accessed, acquired, used or disclosed *without authorization* or for reasons *unrelated to treatment, payment or healthcare operations,* including where an administrative error has led to a *greater than “minimum necessary” use, access or disclosure of PHI.*

**Unsecured PHI** means the PHI was available to an unauthorized individual *without* being first rendered unusable, unreadable, or indecipherable to through the use of encryption or destruction technologies and methodologies.

**Law Enforcement Delay** means a request by law enforcement to delay breach notification for 30 days, or longer if notification would compromise a notification or other law enforcement activity.

**Protected Health Information (PHI) includes:**

* Name
* Street address, city, county, state and zip code
* All elements of dates (except year) for dates directly related to an individual, including date of birth, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into single category of age 90 or older
* Phone numbers
* Fax numbers
* Email addresses
* Social security numbers
* Medical record and account numbers
* Health plan beneficiary numbers
* Certificate/license numbers
* Vehicles identifiers and serial numbers, including license plate numbers
* Device identifiers and serial numbers
* Web Universal Resource Locators (URL’s)
* Internet protocol (IP) address numbers
* Full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).
* Genetic information, such as family history and test results.

**Exceptions to the definition of “breach”:**

1. The unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate
2. The inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate.  In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule

Note: In both of the above situations, the PHI cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

1. The covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information

**Procedures:**

1. Reporting: Staff members must immediately report any actual or potential to the privacy, security or confidentiality of PHI or PI, in any format, to the Compliance Officer.
2. Evaluate and Assess Risks: Upon receiving a report about a potential privacy or security breach, either from a workforce member or a business associate (BA), Company will perform a Risk Assessment to determine whether the affected individual(s) and the Secretary of HHS must be notified.
3. Risk Assessment will include:
	1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
	2. The unauthorized person who used the protected health information or to whom the disclosure was made;
	3. Whether the protected health information was actually acquired or viewed; and
	4. The extent to which the risk to the protected health information has been mitigated.
4. If the Risk Assessment indicates that no exception for reporting the breach exists and the breach must be reported, the Breach Notification Procedure below will be followed.
5. If the Risk Assessment indicates that there is a “low probability of compromise” of the PHI, no notification will be required.
6. If the PHI was secured, through being rendered unusable, unreadable, or indecipherable to through the use of encryption or destruction technologies and methodologies, no breach has occurred and no reporting is required.
7. If the source of the breach was a business associate, Company will hold business associate accountable for providing the information required for the breach notification as outlined below within a reasonable time so Company can meet its obligations to report the breach to the affected individuals within 60 days of the date of the breach.
8. Company will determine whether any other procedures must be followed under applicable state laws. A resource for state security breach notification laws can be found at: <https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html>
9. Company will determine whether law enforcement needs to be notified of the breach.
10. Company will document all risk assessments and the decisions made for notifications and keep records on file for at least 6 years.

**Breach Notification Content for Individuals:**

1. A description of the breach
2. A description of the types of information that were involved in the breach
3. The steps that the affected individual(s) should take to protect themselves from potential harm
4. A brief description of what the covered entity is doing to:
	1. Investigate the breach
	2. Mitigate the harm
	3. Prevent further breaches
	4. Provide contact information at no cost to the individual

**Breach Notification Requirements:**

 **Breaches of Less than Five Hundred (<500) Individuals:**

1. Company will provide the affected individual(s) with a notice in written form by first-class mail, or send an e-mail notice, if the affected individual has agreed to receive such notices electronically. The notice will be provided without unreasonable delay and, in no case, later than sixty (60) days (absent a law enforcement delay) following the discovery of a breach.
2. If there is insufficient or out of date contact information our facility will do the following if the breach involves:
	1. 9 or fewer individuals with out of date or insufficient contact information - Company will notify the individual(s) through an alternative form of written notice, e.g. telephone, website posting or other HHS approved means.
	2. 10 or more individuals with out of date or insufficient contact information - Company will provide the notice on the home page of Company’s website, or provide the notice in major print or broadcast media where the affected individuals most likely reside and a toll-free number or collect call option for individuals to contact Company to get more information about the breach.
3. Company will report the breach to the Secretary of Health & Human Services, within sixty (60) days of the end of the calendar year in which the breaches occurred by filling out the form at <https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true>
4. A separate form will be completed for every breach that occurred during the calendar year.  The electronic form OMB No. 0990-0346 will be completed as posted on the Health & Human Services website. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>

 **Breaches of 500+ Residents within Our State or Jurisdiction:**

1. Company will provide a notice to prominent media outlets, by press release, serving our State or jurisdiction. It will be provided without unreasonable delay and, in no case, later than sixty (60) days (absent a law enforcement delay) following the discovery of the breach and it will include the same information required for the individual notice
2. Company will report the breach to the Secretary of Health & Human Services within sixty (60) days of breach by filling out the form at <https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true>
3. See HHS breach reporting instructions at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>