[Enter Organization Logo]

BREACH OF UNSECURED PHI

Policy Number: [Enter]
Effective Date: [Enter]

HIPAA requires Covered Entities to notify affected individuals, the U.S. Department of Health & Human Services, and, in some cases, the media of a "Breach" of Unsecured PHI. <u>This policy is designed for use by health care providers that qualify as Covered Entities.</u> HIPAA also requires Business Associates to notify the Covered Entity following the Business Associate's discovery of a Breach of Unsecured PHI. *See* 45 C.F.R. § 164.410.

As discussed in Part II below, Minnesota law also requires disclosure of a "breach of the security of the system" in some circumstances. Minn. Stat. § 325E.61.

I. HIPAA Breach Policy:

A. Purpose

[Organization] must comply with rules related to privacy incident response and breach notification. *[Organization]* shall immediately respond to any actual or potential Breach of PHI (a "Privacy Incident") to ensure confidentiality is maintained and to mitigate any adverse effects resulting from the Privacy Incident. Privacy Incidents shall be reported to the Privacy/Security Official immediately for further investigation as outlined below.

B. In General

The Privacy/Security Official shall notify patients (and the Secretary and potentially the media, as described below) of any Breach of Unsecured PHI as required under the Regulations and pursuant to the following procedure:

1. Notification of Privacy/Security Official

Workforce members shall as soon as possible, notify the Privacy/Security Official of any Privacy Incident. The Privacy/Security Official shall ensure that any necessary training occurs so that Workforce members understand their obligations to make such reports to the Privacy/Security Official. The Privacy/Security Official, along with the Response Team, as outlined in Section I.D of this policy (the "Response Team"), will investigate all reports of Privacy Incidents to determine whether the Privacy Incident in fact constitutes a violation of the Privacy Rule (subpart E of 45 C.F.R. part 164).

2. Risk Assessment to Determine Whether the Privacy Incident is a Breach

If the Privacy Incident constitutes a violation of the Privacy Rule, the Privacy/Security Official and the Response Team will conduct a documented risk assessment of the violation to determine if the Privacy Incident meets the regulatory definition of "Breach" or if it can be demonstrated that there is a low probability that the PHI has been compromised based on an analysis of certain factors, as set forth under the Regulations at 45 C.F.R. § 164.402.

3. **Exceptions**

In conducting this analysis, the Privacy/Security Official and Response Team will also determine and document if the violation meets any of the regulatory exceptions to the definition of Breach at 45 C.F.R. § 164.402(1)(i)-(iii). These exceptions include:

> (i) An unintentional acquisition, access, or use of PHI by a Workforce member or person acting under the authority of *[Organization]*, 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.
>
> (ii) Any inadvertent disclosure by a person who is authorized to access PHI at *[Organization]* to another person authorized to access PHI at *[Organization]*, or organized health care arrangement in which *[Organization]* participates, and the information received as a result of such disclosure is not further used or disclosed.
>
> (iii) A disclosure of PHI where *[Organization]* 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.

4. **Risk Assessment Factors**

Except as provided directly above, any unauthorized Use or Disclosure of PHI in violation of the Privacy Rule is presumed to be a Breach. However, the Response Team will conduct a documented risk assessment of the violation to determine if the regulatory definition of "Breach" has been triggered by the Privacy Incident or if it can be demonstrated that there is a low probability that the PHI has been compromised based on an analysis of at least the four factors set forth below. However, additional factors may need to be considered to appropriately assess the risk that the PHI has been compromised, given the circumstances of the impermissible Use or Disclosure, and as determined to be appropriate by the Privacy/Security Official and the Response Team.

- The nature and extent of the PHI involved including the types of identifiers and the likelihood of re-identification. Examples of particularly sensitive data would include a patient's social security number, credit card number, or health history.

- The unauthorized person who used the PHI or to whom the disclosure was made. For example, a recipient who is obligated to abide by HIPAA (e.g., another Covered Entity) generally poses a lower risk of compromising the PHI than someone who has no independent obligations to comply with HIPAA.

- Whether the PHI was actually acquired or viewed. For example, PHI is not actually acquired or viewed when a laptop containing PHI is stolen or lost and a forensic study of the laptop shows that the PHI was never accessed. PHI would be actually acquired or viewed if *[Organization]* mails PHI to the wrong person and the person opens the letter.

- The extent to which the risk to the PHI has been mitigated. For example, there may be a lower risk of compromise if *[Organization]* receives satisfactory assurances from the recipient that there was no further Use or Disclosure of the PHI and that the PHI has been destroyed.

[Organization]'s analysis should include each of the factors discussed above and such other factors as the Privacy/Security Official and the Response Team determine to be necessary. *[Organization]* will then evaluate the overall probability that the PHI has been compromised by considering all factors in combination.

5. **Burden of Proof**

In the event of a Use or Disclosure of PHI in violation of the Privacy Rule, *[Organization]* has the burden of demonstrating that the Use or Disclosure does not constitute a Breach or that all notifications required under HIPAA have been made. *See* 45 C.F.R. § 164.414(b).

6. **Notification to Patients**

If the violation is determined to be a Breach, the Privacy/Security Official will notify each individual whose Unsecured PHI has been, or is reasonably believed by *[Organization]* to have been, accessed, acquired, used, or disclosed, as a result of such Breach. The Privacy/Security Official will provide this notification without unreasonable delay, but in any event within 60 calendar days after the date the Breach was discovered. *[Organization]* shall delay the notification pursuant to a request of law enforcement as described in section 9 below. The Privacy/Security Official shall give notice in the manner described in 45 C.F.R. § 164.404(d) and the notification will contain the following information:

- A brief description of what happened, including the date of the Breach and date of discovery of the Breach, if known;

- 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);

- Any steps the patient(s) should take to protect themselves from potential harm resulting from the Breach;

- A brief description of what *[Organization]* is doing to investigate the Breach, to mitigate harm to patients, and to protect against any further Breaches; and

- Contact procedures for patients to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

7. Notification to the Secretary of Department of Health & Human Services

Following the discovery of a Breach of Unsecured PHI, *[Organization]* must notify the Secretary of the United States Department of Health and Human Services pursuant to 45 C.F.R. § 164.408. For Breaches of Unsecured PHI involving 500 or more individuals, *[Organization]* shall, except pursuant to a delay requested by law enforcement as described in section 9 below, provide notice to the Secretary contemporaneously with the notice to patients discussed above and in the manner specified on the HHS website. For Breaches of Unsecured PHI involving fewer than 500 individuals, *[Organization]* shall maintain a log or other documentation of such Breaches and, not later than 60 days after the end of each calendar year, provide notice to the Secretary of Breaches discovered during the preceding calendar year, in the manner specified on the HHS website. *[Organization]* can make this notification on the HHS Website.

8. Notification to the Media

For any Breach involving more than 500 patients, *[Organization]* must notify the media pursuant to 45 C.F.R. § 164.406. Except pursuant to a delay requested by law enforcement as described in section 9 below, *[Organization]* will provide such notice without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach.

9. Delay Requested by Law Enforcement

If a law enforcement official states to *[Organization]* that a notification, notice, or posting required by this policy would impede a criminal investigation or cause damage to national security, *[Organization]* shall delay such notification, notice, or posting in accordance with this policy and 45 C.F.R. § 164.412.

- If the law enforcement official's statement is in writing and specifies the time for which a delay is required, *[Organization]* will delay such notification, notice, or posting for the time period specified by the official;

- If the law enforcement official's statement is made orally, *[Organization]* will 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 law enforcement official submits a written statement to *[Organization]* during that time.

C. Retention

The Privacy/Security Official shall maintain a log of all risk assessments and breach notifications made by the *[Organization]* pursuant to this policy. The log should maintain documentation that all required notifications were made, or alternatively, of the risk assessment analysis that an impermissible Use or Disclosure did not constitute a Breach in cases where it was determined that a Breach did not occur. All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate all appropriate steps were completed. All supporting documentation associated with the potential Breach shall be maintained for a minimum of six (6) years.

D. Response Team

1. Composition of Response Team

When notified of a Privacy Incident, the Privacy/Security Official shall assemble a Response Team with composition determined by the facts and circumstances of the Privacy Incident. Response Team members shall include the Privacy/Security Official and personnel as determined to be appropriate, which may include:

- Representatives from the location or department where the incident occurred;
- Risk management representative;
- Information technology representative;
- Outside legal counsel and other experts as appropriate.

2. The Response Team Shall Take the Following Actions:

- Create a timeline of events and determine additional facts as necessary;
- Determine response(s) to incident and assign responsibilities and timeframe for completion; and
- Determine if any policies and procedures or processes must be changed to mitigate incident recurrence. Assign responsibility for making changes and follow-up to confirm completion.

E. Miscellaneous

1) The Privacy/Security Official shall maintain files of Privacy Incident Response Team investigations and meetings;

2) The policies and procedures relating to training, complaints, sanctions, refraining from intimidating or retaliatory acts, waiver of rights, policies and procedures and documentation (as required under 45 C.F.R. § 164.530(b), (d), (e), (g), (h), (i) and (j)) apply to the provisions outlined in these Breach Notification Procedures;

3) Capitalized terms not otherwise defined herein shall have the meanings assigned to them in the HIPAA regulations.

II. Breach of the Security of the System Policy:

A person or business that conducts business in Minnesota, must comply with Minnesota law regarding a “breach of the security of the system.” Minn. Stat. § 325E.61. Government entities must comply with similar rules. *See* Minn. Stat. § 13.055. This policy is designed to explain the obligations of non-governmental health care providers. Many other states have similar rules designed to protect residents of those states.

A. Purpose

[Organization] must comply with Minnesota law regarding a “breach of the security of the system.” *[Organization]* shall immediately respond to any actual or potential breach of the security of the system according to the same policies and procedures documented above.

B. In General

The Privacy/Security Official shall notify affected residents of Minnesota (and potentially consumer reporting agencies) of any breach of the security of the system pursuant to the following procedure:

1. Assessment to Determine Whether the Privacy Incident is a Breach of the Security of the System

Following notification of Privacy/Security Official of any Privacy Incident, the Privacy/Security Official, along with the Response Team, will investigate and determine whether the Privacy Incident constitutes a breach of the security of the system as defined in Minnesota Statutes section 325E.61.

2. Definition of Breach of the Security of the System

“Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by *[Organization]*.

3. Exception

Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

4. Definition of Personal Information

The term “personal information” means, when not encrypted, an individual’s first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number;
- Driver's license number or Minnesota identification card number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

5. **Notification to Patients**

If the violation is determined to be a breach of the security of the system, the Privacy/Security Official will notify each Minnesota resident of whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The Privacy/Security Official will provide this notification in the most expedient time possible and without unreasonable delay. *[Organization]* will delay the notification pursuant to a request of law enforcement in accordance with Minnesota Statutes section 325E.61(c). The Privacy/Security Official shall give notice in the manner described in Minnesota Statutes section 325E.61(g).

6. **Notification to Consumer Reporting Agencies**

If *[Organization]* discovers a breach of the security of the system requiring notification of more than 500 persons at one time, *[Organization]* shall also notify, within 48 hours, all major national consumer reporting agencies (as defined in 15 U.S.C. § 1681a(p)) of the timing, distribution, and content of the notices to individuals.