POLK COUNTY BREACH NOTIFICATION POLICY

REFERENCES/CROSS REFERENCES: 45 C.F.R. § 164.402 (Subpart D)

Polk County, Iowa is committed to maintaining the trust, confidence and confidentiality and prevent significant risk of financial, reputational or other harm to Polk County residents who utilize services with Polk County. In order to accomplish this goal it is important that all employees become familiar with proper notification when a suspected or actual breach occurs.

The purpose of this policy is to provide employees with guidance when monitoring and reporting incidents of unauthorized Use, Acquisition, Access or Disclosure of Unsecured PHI.

All employees are required to immediately report all suspected unauthorized acquisition, access, use or disclosures of PHI to the Polk County HIPAA Committee ("Committee"). Employees who use or disclose PHI in violation of the Privacy or Security Rule, or who learn of a violation of the Privacy or Security Rule must notify the Committee. The failure to report a Suspected Breach in a timely manner may result in discipline, including but not limited to termination of employment.

Polk County, Iowa will not retaliate against any employee(s) who report HIPAA violations.

A. Definitions

Breach. A breach is an impermissible acquisition, access, use or disclosure of unsecured PHI that compromises the privacy and/or security of an Individual's protected health information ("PHI").

Business Associate. A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, Polk County. A member of Polk County's workforce is not a business associate. A "business associate" is further defined in 45 C.F.R § 160.103(3).

Breach Requiring Notification. A Breach that meets the criteria specified in this policy and thus requires notification of affected individuals, HHS, and/or the media under applicable federal or state laws.

Discovery Date. Discovery date is (i) for Suspected Breaches reported by a Workforce Member, the date upon which the Workforce Member discovered, or with reasonable diligence would have discovered, the Suspected Breach; or (ii) for Suspected Breaches reported by an agent of the Provider other than a Workforce Member, the date the agent A breach shall be treated as "discovered" as of the first day on which the Breach is known to Polk County employee(s), or, by exercising reasonable diligence would have been known to any person, other than the person committing the breach, who is a Polk County workforce member, or an agency, subcontractor or business associate of Polk County.

HHS. The U.S. Department of Health and Human Services.

HIPAA. The provisions of Privacy Rule (subpart E of 45 CFR part 164 promulgated under the Health Insurance Portability and Accountability Act of 1996), and relevant governmental guidance issued thereunder.

"Inadvertent Disclosure of PHI". When a person authorized to access PHI by the Provider of a Business Associate of the Provider, inadvertently discloses such PHI to another person authorized to access PHI by the Provider or a Business Associate of the provider; and the information is not further used or disclosed in violation of HIPAA.

Law Enforcement Delay. If a law enforcement official determines that a notification, notice or posting required under HIPAA would impede a criminal investigation or cause damage to national security.

Polk County HIPAA Committee. Consists of Privacy Officer, Security Officer, Compliance Officer and Legal Counsel.

Privacy Officer. The Polk County Privacy Officer, or his/her designee.

Privacy Policies. Polk County, Iowa privacy practice policy or policies.

Protected Health Information (PHI). Individually identifiable health information transmitted or maintained in oral, paper, or electronic form (except employment records held by the Polk County, Iowa in its role as an employer).

Suspected Breach. Any circumstances in which the individual or entity suspects that the PHI of Polk County, Iowa client/patient may have been acquired, accessed, used, or disclosed in a manner that is inconsistent with the Polk County, Iowa's Privacy Policies or in violation of any federal or state statute or regulation.

"Unintentional" acquisition, access, or use. When (1) the PHI is acquired, accessed or used by a person acting under the authority of the Provider or a Business Associate of the Provider; (2) the person was acting in good faith and within the scope of his or her authority; and (3) the acquisition, access, or use does not result in further unauthorized use or disclosure.

"Unsecured" Protected Health Information (PHI). Information that is not secured using technology or methodology which renders the information "unusable, unreadable or indecipherable to unauthorized individuals."

Workforce Member. Polk County employee, volunteer, trainee, or other person whose conduct in the performance of work for Polk County, is under the direct control of Polk County, whether or not they are paid by Polk County, Iowa.

B. Breach

A breach does not occur if one of the exceptions applies:

a. Unintentional use, acquisition or access that was done in good faith and does not result in any further violation of the privacy rule (ex: not re-disclosed); or
b. Inadvertent disclosure by an authorized user to another covered entity and it is not used in violation of the privacy rule (ex: not re-disclosed); or
c. Disclosure where Polk County has a good faith belief that an unauthorized person whom the disclosure was made would not be able to retain the information.

C. Presumption of Breach

In none of the exceptions apply, a breach is presumed to occur unless there is a low probability of compromised. Compromised is where there exists a significant risk of financial, reputational or other harm to the individual. Low probability is demonstrated if one of these four (4) factors apply:

a. The nature and extent of PHI disclosed
b. The unauthorized person(s) PHI disclosed to
c. Whether the PHI was acquired or viewed
d. The extent to which the risk was mitigated.

D. Submitting a Suspected Breach Report

All Suspected Breaches must be reported to the Polk County, Iowa HIPAA Committee in writing (Suspected Breach Notification Form – Attachment A) or by telephone or electronic mail immediately, and in no event more than twenty-four (24) hours after the individual or entity became aware of the Suspected Breach.

A suspected breach may be reported anonymously; however, the individual reporting a suspected breach must include enough information to investigate the alleged breach to include information found in the Suspected Breach Notification Form.

E. Risk Assessment and Investigation

Upon receiving a report of a suspected breach, an investigation (Risk Assessment) will immediately occur. The individual who received the initial Suspected Breach report shall complete the Suspected Breach Analysis Form (Attachment B). The Privacy Officer will determine if other individual(s)' assistance is needed to include, but not limited to, Security Officer, Compliance Officer, employee who reported suspected breach, legal counsel, risk management, human resources or outside law enforcement agencies. It is Polk County's expectation that Polk County employees cooperate in a timely manner in the investigation.

The Privacy Officer, Committee or other individual(s)l assisting in the Risk Assessment and Investigation shall conduct an initial review to determine whether immediate steps must be undertaken to mitigate risks associated with a Suspected Breach. If the Suspected Breach may involve criminal activity, the Privacy Officer, in consultation with legal counsel and Risk Management, will contact appropriate law enforcement officials.

The Privacy Officer or Committee or designee shall investigate the Suspected Breach and document relevant information on the Suspected Breach Notification Form.

Polk County will make and retain records of such risk assessment and determinations, including the basis for determinations that unauthorized acquisition, access, Uses or Disclosures are not Breaches of Unsecured PHI for six (6) years.

F. Breach Requiring Notification

A Suspected Breach Requiring Notification occurs if:

a. The information acquired, accessed, used or disclosed is/was PHI (and such PHI was not deidentified, or included in a limited data set from which each individual's date of birth, and zip code or social security number were removed); and
b. The acquisition, access, use, or disclosure of the PHI violated HIPAA; and
c. The PHI was Unsecured PHI at the time of the acquisition, access, use or disclosure.
d. The Suspected Breach poses a significant risk of financial reputation or other harm to the affected individual(s). The following factors are to be considered in determining a significant risk of financial reputation or other harm:
    1. Who impermissibly used or to whom the information was impermissibly disclosed.
    2. Whether immediate steps to mitigate the harm render the risk to the individual to be less than "significant".
    3. Whether impermissibly disclosed PHI was returned prior to it being accessed for an improper purpose.
    4. The type and amount of PHI involved in the impermissible use or disclosure.
    5. None of the following exceptions apply:
        i. The suspected breach was an "unintentional" acquisition, access or use of PHI; or

        ii. The suspected Breach was an "inadvertent disclosure" of PHI; or

        iii. The individual or entity that received the inappropriately disclosed PHI is/was incapable of retaining the information.

G. Notification Procedures

If a breach has occurred, the Privacy Officer will notify the individual(s) whose Unsecured PHI was acquired, accessed, Used or Disclosed improperly using written notice, substitute notice, or notice in urgent situations, as appropriate.

a. <u>Written Notice</u>

Written Notice will be written in plain language and will include, to the extent possible:

1. A brief description of what happened including the date of the breach and the date of discovery of the breach;
2. A description of the types of Unsecured PHI involving (without include the specific PHI);
3. Any steps the individual(s) should take to prevent potential harm resulting from the Breach;
4. A brief description of what Polk County is doing to investigate the Breach, to mitigate harm to Individual(s) and to protect against further Breaches:

5. Contact procedures for Individual(s) to ask questions, learn additional information, to include a toll free telephone number, e-mail address, web site or postal address.

Written notice will be provided without unreasonable delay and in no case later within sixty (60) calendar days after the breach is discovered. A law enforcement delay to prevent crimes is an exception.

Written notification shall be mailed by first-class mail (or electronic mail if the Individual has agreed to electronic mail) to the Individual (or the next of kin of the Individual if the Individual is deceased) at the last known address of the Individual or next of kin or if specified as a preference by the Individual by electronic mail. Notification may be provided in one or more mailings as new information becomes available.

b. Substitute notification. If the contact information is out of date or insufficient (including a phone number, email address, or any other form of appropriate communication) that precludes direct written notification to the Individual, a substitute form of notice shall be provided.

In the case where there are 10 or more Individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period of ninety (90) days on the home page of the County's Web site or conspicuous notice in a major print or broadcast media, including major media in geographic areas where the Individual(s) affected by the breach likely reside. Such media notice or web posting will include:

- A toll-free phone number that remains active for ninety (90) days in order for an Individual to learn whether the Individual's unsecured PHI is possibly included in the breach.

c. Urgent Situations Notice. In any case deemed to require urgency because of possible imminent misuse of unsecured PHI, Polk County, in addition to written notice may provide information to Individuals by telephone or other appropriate means.

H. Breaches Involving 500 or More Individuals.

a. Notice to Media of Breaches (involving more than 500 residents of the same State or jurisdiction).

If a Breach involves more than 500 residents of the same State or jurisdiction, the Privacy Officer or designee(s) will notify the media in accordance with the Breach Notification Requirements. Such notification will be provided without unreasonable delay and in no case later than 60 calendar days after the discovery of the Breach.

b. Notice to Department of Health and Human Services (Office of Civil Rights).

If a Breach involves 500 or more individuals, the Privacy Officer or designee(s) will notify the Department of Health and Human Services in the manner specified in the Breach Notification Requirements on the Department of Health and Human Services website. Such notification will be

provided without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach.

I. Breaches Involving Less Than 500 Individuals.

The Privacy Officer or designee(s) shall maintain a log of Breaches involving less than 500 individuals (Maintenance Log – Attachment C) and, not later than 60 days after the end of the calendar year, shall notify the Department of Human Services in the manner specified in the Breach Notification Requirements and on the Department of Health and Human Services website.

J. *Breaches by Business Associates.*

Polk County's Business Associates are required to monitor and report incidents of unauthorized acquisition, access, Use or Disclosure of Unsecured PHI with respect to PHI the Business Associates acquires, access, Uses or Discloses, in accordance with the Breach Notification Requirements and Business Associate Agreements.

Polk County's Business Associates are required to determine whether incidents of unauthorized, acquisition, access, Use or Disclosure of Unsecured PHI constitute a Breach with respect to PHI the Business Associate or one of its subcontractors acquires, accesses, Use or Discloses, in accordance with the Breach Notification Requirements and Business Associate Agreements.

POLK COUNTY SUSPECTED BREACH NOTIFICATION FORM

Date(s) of Suspected Breach: **Discovery Date:**

_____/_____/_____ to _____/_____/_____ _____/_____/_____

Approximate Number of Individuals Affected: (identify single individual below, for multiple individuals, use Attachment D).

_____, _____

Business Associate: (complete this section if Suspected Breach occurred at or by a Business Associate).

Name: _____

Address: _____State: _____ Zip Code: _____

Business Associate Contact Name: _____

Business Associate Contact: Phone _____ Email _____

Type of Suspected Breach (check all that apply):

____ Theft _____

____ Loss _____

____ Improper Disposal _____

____ Unauthorized Access _____

____ IT Incident _____

____ Other/Unknown (explain) _____

Location of Breach Information (check all that apply):

____ Laptop _____

____ Desktop Computer _____

____ Network Server _____

____ Email _____

____ Other Portable Electronic Device _____

____ Electronic Medical Record _____

____ Paper _____

____ Other (explain) _____

Type of PHI (check all that apply):

____ Demographic Information _____

____ Financial Information _____

____ Clinical Information _____

____ Other (explain) _____

Brief description of the circumstances surrounding the Suspected Breach:

_____

_____

_____

_____

Initial Report submitted by:

_____ on _____/_____/_____ _____

Name Date Contact Information

Initial Report received by:

_____ on _____/_____/_____ _____

Name Date Contact Information

POLK COUNTY BREACH RISK ASSESSMENT FORM

To be completed by Privacy Officer or Compliance Committee. If Compliance Committee, each individual should independently complete form and meet to discuss their findings)

Date/Description of Incident:

_____

_____

_____

Factors to Consider:

1) What is the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification? (Individual names, addresses, identification numbers, discharge dates, diagnoses, specificity of diagnosis, size of community served, whether the unauthorized recipient may have the ability to combine the information with other available information to re-identify the Individuals.

_____

_____

_____

2) Who is the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made? (Another HIPAA-regulated entity, a federal entity obligated to comply with the Privacy Act of 1974 or Federal Information Security Management Act of 2002, Individual's employers.

_____

_____

_____

3) Have you investigated the impermissible use or disclosure to determine if the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed? (laptop computer – was it stolen and later recovered and forensic analysis show the PHI on computer never accessed, viewed, acquired, transferred or otherwise compromised though the opportunity existed or information was encrypted; if information mailed to wrong Individual – did they return without opening envelope, did they notify you that they received envelope opened and read information).

_____

_____

_____

4) What is the extent to which the risk to the PHI has been mitigated?

[ ] low probability that the data has been compromised

[ ] was the information destroyed

[ ] possibility of harm or future harm to Individual's reputation, financial

[ ] assurance of an employee, affiliated entity, business associate or another covered entity that the entity or person destroyed the information received in error (such assurances from other third parties may not be sufficient)

_____

_____

_____

5) Safeguards in Place Prior to the Breach (check all that apply):

____ Firewalls	_____
____ Packet Filtering	_____
____ Secure Browser Sessions	_____
____ Passwords	_____
____ Encrypted Wireless	_____
_____Physical Security	_____
____ Anti-Virus Software	_____
____ Intrusion Detection	_____
____ Biometrics	_____
____ Other (please explain)	

6) Other factors relevant to analysis of incident?

_____

_____

_____

Conclusion based on consideration of factors: Is there a very low probability of compromise?

[ ] Yes. Please explain.

_____

_____

_____

[ ] No. Breach notification required.

Completed by: _____

Title: _____

Date: _____

Attachment B

Breach Maintenance Log

Date of Breach	Discovery Date	No. of Affected Individuals	Date HHS Notified	Staff Member	Comments	Date Media Notified
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___
___/___ ___	___/___ ___		___/___/ ___			___/___ ___

ATTACHMENT "C"

List of Affected Individual

_____ Affected Group

_____/_____/_____ Date of Suspected Breach

_____/_____/_____ Discovery Date

Last Name	First Name	Ident. No.	Contact Attempts	By:	Comments	Written Notice	Sent By:
			__/__/__			__/__	
			__/__/__			__/__	
			__/__/__			__/__	
			__/__/__			__/__	
			__/__/__			__/__	
			__/__/__			__/__	
			__/__/__			__/__	
			__/__/__			__/__	
			__/__/__			__/__	
			__/__/__			__/__	
			__/__/__			__/__	

ATTACHMENT "D"