



ESSENT HEALTHCARE, INC.

Section:	HIPAA Privacy	Effective Date:	9/23/09
Subject:	Reporting of Data Breaches	Revision Date:	10/31/09
Policy #:	HIPAA-017	Review Date:	10/31/09
Responsible Party:	Corporate Compliance Officer	Revision #:	2

Scope:

This policy applies to all workforce members and all Business Associates of Essent Healthcare, Inc., (“Essent”).

Purpose:

The purpose of this policy is to set forth the requirements for reporting of certain data breaches to the Privacy Officer.

Policy:

It is the policy of Essent Healthcare, Inc. that all data breaches (as defined below) shall be reported to the Hospital Privacy Officer and the Corporate Compliance Officer as outlined below. In addition, data breaches shall be reported to the affected individual, local media, and to the Secretary of HHS as outlined below.

Definitions:

Breach of Unsecured Information – The unauthorized acquisition, access, use, or disclosure of unsecured protected health information which compromises the privacy or security of the protected health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. A breach is considered discovered when the incident becomes known to the covered entity, not when the covered entity concludes its analysis as described below.

Unsecured Protected Health Information – Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology such as encryption and/or document destruction. Unsecured protected health information can include information in any form or medium including electronic, paper, or oral form.

Encryption – Electronic protected health information is considered to be encrypted when an algorithmic process is used to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or “key” and such confidential process or key that might enable decryption has not been breached.



ESSENT HEALTHCARE, INC.

Section:	HIPAA Privacy	Effective Date:	9/23/09
Subject:	Reporting of Data Breaches	Revision Date:	10/31/09
Policy #:	HIPAA-017	Review Date:	10/31/09
Responsible Party:	Corporate Compliance Officer	Revision #:	2

Unauthorized Acquisition, Access, Use, or Disclosure – An impermissible use or disclosure of protected health information under the HIPAA Privacy Rule.

Compromises the privacy or security of protected health information – Poses a significant risk of financial, reputational, or other harm to the individual whose data has been breached.

Procedures:

1. All breaches of unsecured protected health information shall be reported to the Hospital Privacy Officer immediately upon discovery. This includes reporting the loss or theft of any portable device (laptop, PDA, smart-phone, etc...) that may contain confidential company information or protected health information. Breaches involving encrypted information need not be reported.
2. Following the report of any data breach, the Hospital Privacy Officer shall notify the Corporate Compliance Officer and begin an investigation to determine whether further notifications are necessary.
 - a. Determine whether the use/disclosure violates the privacy rule (an impermissible use or disclosure of protected health information under the Privacy Rule).
 - b. Perform a risk assessment to determine whether the violation compromises the privacy or security of the protected health information and/or poses a significant risk of financial, reputational, or other harm to the individual who is the subject of the information. If the nature of the protected health information does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach and no further notification is required.
 - c. Determine whether the incident falls under one of the exceptions described below.
 - d. Document risk assessment such that it can be demonstrated, if necessary, that no breach notification was required following an impermissible use/disclosure of protected health information. Risk assessments shall be maintained for seven years.
3. Determine whether an exception to the breach notification requirements applies. The



ESSENT HEALTHCARE, INC.

Section:	HIPAA Privacy	Effective Date:	9/23/09
Subject:	Reporting of Data Breaches	Revision Date:	10/31/09
Policy #:	HIPAA-017	Review Date:	10/31/09
Responsible Party:	Corporate Compliance Officer	Revision #:	2

following do not constitute a breach:

- a. Unintentional acquisition, access, or use of protected health information by a workforce member of the Hospital or its Business Associate. For example, the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of the covered entity, if the acquisition, access, or use was made in good faith, within the course and scope of employment, and does not result in further disclosure (i.e. nurse accessing the wrong electronic medical record by mistake).
 - b. Inadvertent disclosure of protected health information from one person authorized to access protected health information at a covered entity to another person authorized to access protected health information at the same covered entity.
 - c. Unauthorized disclosures in which the unauthorized person to whom protected health information is disclosed would not reasonably have been able to retain the information. For example, a covered entity sends a number of patient bills to the wrong address. A few of the bills are returned by the post office, unopened, as undeliverable. *Note – the billing statements that were not returned would be treated as potential breaches.*
4. When the risk assessment reveals that a breach has in fact occurred, the covered entity must notify each individual whose unsecured protected health information has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of such breach. Such notification shall be made within 60 days of the discovery of the breach incident. Therefore, all Essent workforce members and Business Associates are required to report known or suspected data breaches to the Privacy Officer immediately.
5. Breach notifications shall, to the extent possible, include the following:
- a. A brief description of what happened, including the date of the discovery of the breach, if known.
 - b. A description of the types of unsecured protected health information that were involved in the breach (such as full name, social security number, date of birth, home address, or other types of information). Covered entities should not include a listing of the actual protected health information that was breached (e.g., list in notice the individual's social security number that was breached).
 - c. Any steps individuals should take to protect themselves from potential harm resulting



ESSENT HEALTHCARE, INC.

Section:	HIPAA Privacy	Effective Date:	9/23/09
Subject:	Reporting of Data Breaches	Revision Date:	10/31/09
Policy #:	HIPAA-017	Review Date:	10/31/09
Responsible Party:	Corporate Compliance Officer	Revision #:	2

from the breach.

- d. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to the individual, and to protect against any further breaches.
- e. Contact information for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, web site, or postal address.
- f. To satisfy this requirement, the covered entity should write the notice at an appropriate reading level, using clear language and syntax, and not include any extraneous material that might diminish the message it is trying to convey. This may include translation into frequently encountered languages, making the notice available in Braille, large print, or audio.

6. The method of notification shall be as follows:

- a. In written form by first class mail at the last known address of the individual.
- b. If the individual is deceased, notice must be sent to next of kin or personal representative.
- c. If the covered entity does not have sufficient contact information for some or all of the affected individuals, or if some of the notices are returned as undeliverable, the covered entity must provide substitute notice for the unreachable individuals. Substitute notice shall be provided as soon as reasonably possible after the covered entity is aware that it has insufficient or out-of-date contact information for one or more affected individuals. The substitute notice must contain all of the elements of the original notice.
- d. If there are fewer than 10 individuals for whom the covered entity has insufficient or outdated contact information to provide written notice, the covered entity can provide substitute notice via telephone, email, or other means.
- e. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, then the covered entity must provide substitute notice through either a conspicuous posting for 90 days on the home page of its web site or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. In addition, substitute notice through web site or other media for 10 or more individuals requires that the covered entity have a toll-free phone number, active for 90 days, where an individual can learn whether the individual's unsecured protected health information may be included in the breach. The toll-free number must be included in the substitute notice. Note: covered entities with out-of-



ESSENT HEALTHCARE, INC.

Section:	HIPAA Privacy	Effective Date:	9/23/09
Subject:	Reporting of Data Breaches	Revision Date:	10/31/09
Policy #:	HIPAA-017	Review Date:	10/31/09
Responsible Party:	Corporate Compliance Officer	Revision #:	2

date information for some individuals can attempt to update the contact information so that they can provide direct written notification, in order to limit the number of individuals for whom substitute notice is required and, thus, potentially avoid the obligation to provide substitute notice through a web site or major print or broadcast media.

7. Notification to the Secretary of the Department of Health and Human Services – Covered entities are required to notify the Secretary of breaches of unsecured protected health information.
 - a. For breaches involving 500 or more individuals, covered entities are required to notify the Secretary immediately. For purposes of this paragraph, the term “immediately” requires that notification be sent to the Secretary concurrently with the notification sent to the individuals which must be sent no later than 60 days after discovery of the breach.
 - b. For breaches involving less than 500 individuals, covered entities may maintain a log of such breaches and annually submit such log to the Secretary documenting the breaches occurring during the preceding calendar year. This notification must be made no later than 60 days from the end of each calendar year.
 - c. Covered entities must maintain annual logs documenting data breaches for submission to the Secretary. The logs must be based on a calendar year and be retained for a minimum of seven years.

References:

FR August 24, 2009; 42740 – Breach Notification Interim Final Rule

Addendum A – for Massachusetts Hospitals Only



ESSENT HEALTHCARE, INC.

Section:	HIPAA Privacy	Effective Date:	9/23/09
Subject:	Reporting of Data Breaches	Revision Date:	10/31/09
Policy #:	HIPAA-017	Review Date:	10/31/09
Responsible Party:	Corporate Compliance Officer	Revision #:	2

Because the State Laws of Massachusetts are more stringent than HIPAA in certain cases, the Massachusetts State Law over-rides HIPAA in certain cases. Below are the requirements for Massachusetts Hospitals:

1. All known or suspected data breaches, involving PHI or other confidential information, must be reported to the Hospital Privacy Officer immediately. For purposes of the Massachusetts policy, the term “*data breach*” shall mean the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth.
2. The Hospital Privacy Officer shall contact the Corporate Compliance Officer to discuss the case and determine how to proceed.
3. Note that the “harm threshold” that must be met for HIPAA purposes does not exist in Massachusetts State Law. Therefore all data breaches are potentially subject to reporting requirements.
4. If a Massachusetts Hospital knows or has reason to know of a breach of security involving any resident of the Commonwealth, or that confidential Hospital information related to a resident of the Commonwealth has been used inappropriately, the Hospital must
 - a. Notify the individual(s) whose information was breached. Notice to individuals shall include, but not be limited to, the individual’s right to obtain a police report, how the individual can request a security freeze and the necessary information to be provided when requesting a security freeze, and any fees required to be paid to any of the consumer reporting agencies. Resident notification, *may not include* the nature of the breach or unauthorized acquisition or use or the number of residents of the Commonwealth were affected by the breach or unauthorized use/access.
 - b. Notify the Attorney General of the Commonwealth. Notification to the Attorney General shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the Commonwealth affected



ESSENT HEALTHCARE, INC.

Section:	HIPAA Privacy	Effective Date:	9/23/09
Subject:	Reporting of Data Breaches	Revision Date:	10/31/09
Policy #:	HIPAA-017	Review Date:	10/31/09
Responsible Party:	Corporate Compliance Officer	Revision #:	2

by such incident at the time of the notification, and any steps that the Hospital has taken or plans to take relating to the incident.

- c. Notify the Director of Consumer Affairs and Business Regulation. Notification to the Director of Consumer Affairs and Business Regulation shall include , but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the Commonwealth affected by such incident at the time of the notification, and any steps that the Hospital has taken or plans to take relating to the incident.