BREACH NOTIFICATION – PROTECTED HEALTH INFORMATION POLICY

Disclaimer

This document is Copyright 2009 by HIPAA Collaborative of Wisconsin (“HIPAA COW”). It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided “as is” without any express or implied warranty. This document is for educational purposes only and does not constitute legal advice. If you require legal advice, you should consult with an attorney.

State Preemption Issues:

There have been no preemption issues identified for covered entities with regard to Wisconsin breach notification laws. However, covered entities may have to review the specific breach notification laws of other states in which they do business or their patients/clients reside. In addition, covered entities may have other federal or state statutory, regulatory or contractual requirements to notify of breaches that should be reviewed.

Purpose: To provide guidance for breach notification by covered entities when impermissive or unauthorized access, acquisition, use and/or disclosure of the organization’s patient protected health information occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule is effective September 24, 2009 with full compliance required by February 22, 2010.1

Background:

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities may have chosen to include notification as part of the mitigation process. HITECH does require notification of certain breaches of unsecured PHI to the following: individuals, Department of Health and Human Services (HHS), and the media. The effective implementation for this provision is September 23, 2009 (pending publication HHS regulations).

Attachments:
- Examples of Breaches of Unsecured Protected Health Information
- Breach Penalties
- Sample Notification Letter to Patients
- Sample Notification Letter to Secretary of Health & Human Services
- Sample Media Notification Statement/Release
- Sample Talking Points
- Examples of Violations and Notification Recommendations
- Sample Breach Notification Log
- Risk Assessment Analysis Tool

Definitions:

Access: Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. ²

Breach: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purpose of this definition, “compromises the security or privacy of the PHI” means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at §164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI.

Breach excludes:
1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) 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 in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care

² 45 CFR § 164.304.
arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

3. A disclosure of PHI where a CE or BA 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.³

Covered Entity: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.⁴

Disclosure: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.⁵

Individually Identifiable Health Information: That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.⁶

Law Enforcement Official: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.⁷

Organization: For the purposes of this policy, the term “organization” shall mean the covered entity to which the policy and breach notification apply.

Protected Health Information (PHI): Protected health information means individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.⁸

Unsecured Protected Health Information: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under section

³ ARRA/HITECH Title XIII Section 13400; §164.402.
⁴ 45 CFR § 160.103.
⁵ 45 CFR § 160.103.
⁶ 45 CFR § 164.503.
⁷ 45 CFR § 164.103.
⁸ 45 CFR § 164.503.
13402(h)(2) of Pub. L.111-5 on the HHS website.

1. Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.
   A. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
   B. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.

2. The media on which the PHI is stored or recorded has been destroyed in the following ways:
   A. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
   B. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Workforce: Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Policy Statement/s:

1. Discovery of Breach: A breach of PHI shall be treated as “discovered” as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to the organization (includes breaches by the organization’s business associates). The organization shall be deemed to have knowledge of a breach if

---

9 45 CFR Parts 160 and 164; Final Rules Issued 8/19/09.
10 HHS issued guidance on protecting personally identifiable healthcare information; document was the work of a joint effort by HHS, its Office of the National Coordinator for Health Information Technology and Office for Civil Rights, and the CMS (Issued 4/17/09).
11 45 CFR § 164.103.
such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (business associate) of the organization (see attachment for examples of breach of unsecured protected health information). Following the discovery of a potential breach, the organization shall begin an investigation (see organizational policies for security incident response and/or risk management incident response), conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to by the organization to have been, accessed, acquired, used, or disclosed as a result of the breach. The organization shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

2. Breach Investigation: The organization shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.\(^{12}\)

3. Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements, the organization will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure.\(^{13}\) The organization shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the organization will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

\(^{12}\) 45 CFR §164.530(jj)(2).

\(^{13}\) The organization may choose to make the decision to notify patients of a breach even after completion of the risk assessment indicates that there is no requirement to do so under ARRA/HITECH.
A. Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
B. The type and amount of PHI involved.
C. The potential for significant risk of financial, reputational, or other harm.

4. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the organization involved or the business associate involved. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:
   A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
   B. If the statement is made orally, document the statement, including the identify 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 written statement as described above is submitted during that time.  

6. Content of the Notice: The notice shall be written in plain language and must contain the following information:
   A. A brief description of what happened, including the date of the breach and 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 whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
   C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
   D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
   E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

---

14 45 CFR § 164.412.
7. Methods of Notification: The method of notification will depend on the individuals/entities to be notified. The following methods must be utilized accordingly:

A. Notice to Individual(s): Notice shall be provided promptly and in the following form:

1. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the organization knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.

2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

   a. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

   b. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the organization’s website, or a conspicuous notice in a major print or broadcast media in the organization’s geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

3. If the organization determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

B. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.

C. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in
which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.\footnote{15}

1. For breaches involving 500 or more individuals, the organization shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.

2. For breaches involving less than 500 individuals, the organization will maintain a log of the breaches and annually submit the log to the Secretary of HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.\footnote{16}

8. \textbf{Maintenance of Breach Information/Log}: As described above and in addition to the reports created for each incident, the organization shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected.\footnote{17} The following information should be collected/logged for each breach (see sample Breach Notification Log):

   A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, 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, account number, etc.).

   C. A description of the action taken with regard to notification of patients regarding the breach.

   D. Resolution steps taken to mitigate the breach and prevent future occurrences.

9. \textbf{Business Associate Responsibilities}: The business associate (BA) of the organization that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the organization of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach.\footnote{18} The BA shall provide the organization with any other available information that the

\footnote{15}{Note: If the breach involves “secured” PHI, no notification needs to be made to HHS.}
\footnote{16}{For calendar year 2009, the organization is required to submit information to the HHS secretary for breaches occurring after the September 23, 2009 effective implementation date.}
\footnote{17}{The organization shall delegate this responsibility to one individual (e.g., Privacy Officer).}
\footnote{18}{Business associate responsibility under ARRA/HITECH for breach notification should be included in the organization’s business associate agreement (BAA) with the associate (See www.hipaacow.org for BAA information).}
organization is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the organization will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is still the burden of the Covered Entity to document this notification).

10. Workforce Training: The organization shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.

11. Complaints: The organization must provide a process for individuals to make complaints concerning the organization’s patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about the organization’s breach notification processes.\(^{19}\)

12. Sanctions: The organization shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

13. Retaliation/Waiver: The organization may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The organization may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

**Applicable Federal/State Regulations:**
- ARRA Title XIII Section 13402 – Notification in the Case of Breach
- FTC Breach Notification Rules - 16 CFR Part 318
- 45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules
- WI § 134.98 – Notice of Unauthorized Acquisition of Personal Information (Note: Not applicable to Covered Entities Under HIPAA).

**Reviewed By:** HIPAA COW Privacy and Security Networking Groups

**Workgroup Members:**
- Julie Coleman, Privacy Officer, Group Health Cooperative of South Central Wisconsin (GHC-SCW)

\(^{19}\) The organization may want to consider adding this right to complaint about the breach notification process to their Notice of Privacy Practices.
Based on ARRA/HITECH Interim Rules – August 24, 2009

- Nancy Davis, Director of Privacy, Ministry Health Care
- Chris DuPrey, Caris Innovation
- Claudia Egan, JD, Von Briesen & Roper, S.C.
- Mary Evans, Meriter Health Services
- Heather Fields, Reinhart Boerner Van Deuren, S.C.
- Bill French, Marshfield Clinic/Ministry Health Care
- Monica Hocum, JD, Hall, Render, Killian, Heath & Lyman, P.C
- Kathy Johnson, Privacy & Compliance Officer, Wisconsin Dept. of Health Services
- Carla Jones, JD, Privacy Officer, Marshfield Clinic
- Sarah Kleaveland-Kupczak, Wheaton Franciscan
- Chrisann Lemery, Compliance Specialist, WEA Trust Insurance
- L. Allen Mundt, Infrastructure Administrator, IT Division, DOA, Waukesha County Government
- Holly Schlenvogt, Privacy Officer, ProHealth Care
- Peg Schmidt, Privacy Officer, Aurora Health Care
- Jim Sehloff, Caretech Solutions, Holy Family Memorial Medical Center
- Charlotte Silvers, RHIA, Jefferson County HIPAA Officer
- Teresa Smithrud, Mercy Health System
- Matthew Stanford, Associate Counsel, Wisconsin Hospital Association
- Jodie Swoboda, North Central Health Care
- Sue Sullivan, Assistant Administrator Patient Care Services, Vernon Memorial Healthcare
- Kerry Taylor, Privacy Officer, Saint Vincent’s Hospital
- Carol Weishar, Aurora Advanced Healthcare
- Kirsten Wild, Sinaiko Healthcare Consulting, Inc.
- Barbara Zabawa, JD, Whyte Hirschboeck, Dudek, S.C.
ATTACHMENTS

Examples of Potential Breaches of Unsecured Protected Health Information

Note: Each of these events may not rise to the level of a “breach.” This can only be determined by completing the risk assessment analysis and making a determination of whether or not there was “harm” to the individual.

- Workforce members access the electronic health records of a celebrity who is treated within the facility.
- Stolen lost laptop containing unsecured protected health information.
- Papers containing protected health information found scattered along roadside after improper storage in truck by business associate responsible for disposal (shredding).
- Posting of patient’s HIV+ health status on Facebook by a laboratory tech who carried out the diagnostic study.
- Misdirected e-mail of listing of drug seeking patients to an external group list.
- Lost flashdrive containing database of patients participating in a clinical study.
- EOB (Explanation of Benefits) sent to wrong guarantor.
- Provider accessing the health record of divorced spouse for information to be used in a custody hearing.
- Workforce members accessing electronic health records for information on friends or family members out of curiosity/without a business-related purpose.
- EMT takes a cell phone picture of patient following a MVA and transmits photo to friends.
- Misfiled patient information in another patient’s medical records which is brought to the organization’s attention by the patient.
- Medical record copies in response to a payers request lost in mailing process and never received.
- Misdirected fax of patient records to a local grocery store instead of the requesting provider’s fax.
- Briefcase containing patient medical record documents stolen from car.
- PDA with patient-identifying wound photos lost.
- Intentional and non-work related access by staff member of neighbor’s information.
- Medical record documents left in public access cafeteria.
Breach Penalties

Penalties for Breach: Penalties for violations of HIPAA have been established under HITECH as indicated below. The penalties do not apply if the organization did not know (or by exercising reasonable diligence would not have known) of the violation or if the failure to comply was due to a reasonable cause and was corrected within thirty days. Penalties will be based on the organization’s culpability for the HIPAA violation. The Secretary of HHS will base its penalty determination on the nature and extent of both the violation and the harm caused by the violation. The Secretary still will have the discretion to impose corrective action without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) that such person committed a violation.

The maximum penalty is $50,000 per violation, with a cap of $1,500,000 for all violations of an identical requirement or prohibition during a calendar year.

The minimum civil monetary penalties are tiered based upon the entity's perceived culpability for the HIPAA violation, as follows:

**Tier A – If the offender did not know**
- $100 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $25,000.

**Tier B – Violation due to reasonable cause, not willful neglect**
- $1,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $100,000.

**Tier C – Violation due to willful neglect, but was corrected.**
- $10,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $250,000.

**Tier D – Violation due to willful neglect, but was NOT corrected.**
- $50,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $1,500,000.

---

20 See HIPAA Enforcement Rule, 45 CFR Part 160, Subpart D, and 42 CFR 1320d-5 as Amended by ARRA Section 13410(d)(3).
Sample Notification Letter to Patients – Document to be Reviewed and Customized Prior to Use

[Date]

[Name here]
[Address 1 Here]
[Address 2 Here]
[City, State Zip Code]

Dear [Name of Organization Patient or Patient Name]:

I am writing to you with important information about a recent breach of your personal information from [Name of Organization]. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include the following information:

A. A brief description of what happened, including the date of the breach and 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 whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Other Optional Considerations:
To help ensure that this information is not used inappropriately, [Name of Organization] will cover the cost for one year for you to receive credit monitoring. To take advantage of this offer, [Need to document the process for how this would work].

We also advise you to immediately take the following steps:

- Call the toll-free numbers of anyone of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

  - **Equifax**: 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241.
  - **Experian**: 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, TX 75013.
  - **TransUnion**: 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. [Name of Organization] apologizes for the stress and worry this situation has caused you and is doing everything it can to rectify the situation.

We have established a toll-free number to call us with questions and concerns about the loss of your personal information. You may call [Insert Toll Free Number] during normal business hours with any questions you have.

We have also established a section on our Web site with updated information and links to Web sites that offer information on what to do if your personal information has been compromised.

[Insert Closing Paragraph Based on Situation]
Sincerely,

[Insert Applicable Name/Contact Information]
Sample Notification Letter to Secretary of Health & Human Services – Document to be Reviewed and Customized Prior to Use

[Date]

Secretary of Health & Human Services
The U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201
Telephone: 202-619-0257
Toll Free: 1-877-696-6775

Dear Secretary:

In compliance with the American Recovery and Reinvestment Act of 2009 (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH), we are notifying you of a recent breach of unsecured protected health information (PHI). The breach involved [Insert Number] patients. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include the following information as communicated to the victims:

A. A brief description of what happened, including the date of the breach and 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 whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

On behalf [Insert Name of Organization] I am communicating this information to you in compliance with ARRA/HITECH.
If you have any questions or require further information, please contact me at [Insert Contact Information].

Sincerely,

[Insert Applicable Name/Contact Information]
Sample Media Notification Statement/Release – Document to be Reviewed and Customized Prior to Use

[Insert Date]

Contact: [Insert Contact Information Including Phone Number/E-Mail Address]

IMMEDIATE RELEASE

[INSERT NAME OF ORGANIZATION] NOTIFIES PATIENTS OF BREACH OF UNSECURED PERSONAL INFORMATION

[Insert Name of Organization] notified [Insert Number] patients of a breach of unsecured personal patient protected health information after discovering the following event:

Describe event and include the following information as communicated to the victims:

A. A brief description of what happened, including the date of the breach and 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 whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

In conjunction with local law enforcement and security experts, [Name of Organization] is working to notify impacted patients to mitigate the damages of the breach. [Name of Organization] has in place safeguards to ensure the privacy and security of all patient health
information. As a result of this breach, steps are underway to further improve the security of its operations and eliminate future risk.

In a notification to patients, [Name of Organization] has offered their resources as well as …. [Insert as Applicable]. [Name of Organization] also has encouraged its patients to contact their financial institutions to prevent unauthorized access to personal accounts.

[Name of Organization] has trained staff available for patients to call with any questions related to the data breach. Patients may call [Insert Phone Number Here] from [Insert Hours] with any questions. In addition, patients may visit [Name of Organization’s] Web site at [Insert Web Address] for further information.

[Name of Organization] understands the importance of safeguarding our patients’ personal information and takes that responsibility very seriously,” said [Insert Name], President and CEO. “We will do all we can to work with our patients whose personal information may have been compromised and help them work through the process. We regret that this incident has occurred, and we are committed to prevent future such occurrences. We appreciate our patients support during this time.

Please direct all questions to [Enter Contact Information].

Sample Talking Points (Based on an Example) – Document to be Reviewed and Customized Prior to Use

Talking Points to Respond to Inquiries About Breach of Unsecured Patient Protected Health Information

What Happened

Describe Incident Objectively (see sample below).

- An employee of the [Insert Name of Organization] has been arrested for using the personal health information of XX patients to obtain loans and credit cards.

- The employee has been charged with identity theft, bank fraud, and credit card fraud.
• **The employee also illegally obtained $XXXXX in reimbursement for fraudulent health claims he/she submitted.**

• **The employee allegedly also sold the personal information of our patients to her brother. He also has allegedly obtained credit cards using the patients’ identities.**

• [Insert Law Enforcement Agency Name] is investigating in order to identify the patients affected by the identity theft.

• **The employee worked as a supervisor in our claims administration area.**

• **The employee has been suspended without pay. Her access to [Insert Name of Organization] facilities and any [Insert Name of Organization] computer systems has been terminated.**

• **As a supervisor, the employee had access to personal information of [Insert Name of Organization] patients.**

• **Her access to patient information was based on her ability to do the job she was assigned.**

• **The employee has been with the [Insert Name of Organization] for XX years.**

• **The employee underwent a full background check, including criminal check, upon her hire in 20XX.**

• **There have been no other charges against this employee in her time at [Insert Name of Organization].**

• **This is the first and only time this type of situation has happened at [Insert Name of Organization].**

• **[Insert Name of Organization] has contacted the affected patients and has provided credit monitoring services and a contact for additional guidance.**

**What Are We Doing Now**

Customize as Applicable

• We are notifying each individual patient that has been affected by the incident and offering resources to answer any questions or concerns that he or she may have about the current situation.
• We are contacting the Secretary of the Department of Health & Human Services to notify her of the breach.

• We are working with our Compliance Department, IT Department, Legal Department, and Human Resources, to review procedures to see if there are additional safeguards we should implement to prevent this type of action in the future.

• We are working with the law enforcement officials to provide them with any information to expedite the investigation and prosecution of this matter.

What We Will Do for Our Patients

• We will continue to make our compliance department available if patients have any questions or concerns regarding their credit.

• We have established a special toll-free number for [Insert Name of Organization] patients to call who have questions regarding their personal information.

• We will also encourage patients to contact any of the three credit reporting agencies and establish a fraud alert.

Examples of Violations and Notification Recommendations

<table>
<thead>
<tr>
<th>Type of HIPAA Violation</th>
<th>Notify Pt?*</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHI mistakenly faxed to a grocery store (ex. prescription, test results)</td>
<td>Yes</td>
</tr>
<tr>
<td>PHI mistakenly faxed to an incorrect pharmacy</td>
<td>Not Required</td>
</tr>
<tr>
<td>Lab results sent to incorrect provider at non-[org] facility</td>
<td>Not Required</td>
</tr>
<tr>
<td>Lab results sent to incorrect provider at [org] facility</td>
<td>Not Required</td>
</tr>
<tr>
<td>Test results faxed to provider's former organization</td>
<td>Not Required</td>
</tr>
<tr>
<td>Lab requisition provided to wrong patient (other patient name on form)</td>
<td>Yes</td>
</tr>
<tr>
<td>Lab requisition provided to wrong patient, but was retrieved before the patient was able to view the other patient's name/information</td>
<td>Not Required</td>
</tr>
<tr>
<td>Paperwork for two other patients provided to patient.</td>
<td>Yes</td>
</tr>
<tr>
<td>EOB (Explanation of Benefits) sent to wrong guarantor</td>
<td>Yes</td>
</tr>
<tr>
<td>Claim sent to known terminated insurance company</td>
<td>Not Required</td>
</tr>
<tr>
<td>Medical record copies in response to a payers request was sent to an incorrect payer, lost in mailing process, and never received or returned</td>
<td>Yes</td>
</tr>
<tr>
<td>Incorrect patient's immunization sent to a parent</td>
<td>Yes</td>
</tr>
<tr>
<td>Event</td>
<td>Compliance</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Surgical order sent to incorrect facility</td>
<td>Not Required</td>
</tr>
<tr>
<td>Provider called own spouse (also a provider) and discussed PHI of patient who may not be a shared patient</td>
<td>Not Required</td>
</tr>
<tr>
<td>Provider verbally informed adult patient's mother of test results</td>
<td>Yes</td>
</tr>
<tr>
<td>Child's visit shared with father's girlfriend</td>
<td>Yes</td>
</tr>
<tr>
<td>Scheduler informed a patient of another patient's name who was treated for mental health, HIV, STDs, etc.</td>
<td>Yes</td>
</tr>
<tr>
<td>Scheduler informed a patient of another patient's name who was seen at a non-specialized facility</td>
<td>Not Required</td>
</tr>
<tr>
<td>Info given to a family member without a password (for a patient who requested restricted access)</td>
<td>Yes</td>
</tr>
<tr>
<td>EMT takes a cell phone picture of patient following a MVA and transmits photo to friends or posts on Facebook</td>
<td>Yes</td>
</tr>
<tr>
<td>Medical record documents left in cafeteria used by the public</td>
<td>Yes</td>
</tr>
<tr>
<td>Paperwork for patients left lying in patient's room &amp; found by someone other than that patient</td>
<td>Yes</td>
</tr>
<tr>
<td>Patient's name and type of services announced in a patient waiting area - other patients present</td>
<td>Yes</td>
</tr>
<tr>
<td>Can hear patient names &amp; DOB in waiting area</td>
<td>Not Required</td>
</tr>
<tr>
<td>Briefcase containing patient medical record documents stolen</td>
<td>Yes</td>
</tr>
<tr>
<td>Lab result printed in incorrect department</td>
<td>Not Required</td>
</tr>
<tr>
<td>Lab results sent by [org] Hospital to [org] Clinic in error (or another entity in the OHCA)</td>
<td>Not Required</td>
</tr>
<tr>
<td>Papers containing PHI found scattered along roadside after improper storage in truck by business associate responsible for disposal (shredding)</td>
<td>Yes</td>
</tr>
<tr>
<td>Transcription documents improperly disposed of at an employee's residence</td>
<td>Yes</td>
</tr>
<tr>
<td>User mistakenly types an incorrect mrn# and immediately exits record</td>
<td>Not Required</td>
</tr>
<tr>
<td>User inappropriately accesses family members' PHI - not legal rep</td>
<td>Yes</td>
</tr>
<tr>
<td>User inappropriately accesses family members' PHI - legal rep</td>
<td>Yes</td>
</tr>
<tr>
<td>User inappropriately accesses neighbors' PHI</td>
<td>Yes</td>
</tr>
<tr>
<td>User inappropriately accesses celebrity’s’ PHI</td>
<td>Yes</td>
</tr>
<tr>
<td>Temporary agency employee accessed father’s record in EHR</td>
<td>Yes</td>
</tr>
<tr>
<td>Posting of patient’s HIV+ health status on Facebook by a laboratory tech who carried out the diagnostic study</td>
<td>Yes</td>
</tr>
<tr>
<td>Unencrypted flashdrive lost that contains database of patients participating in a clinical study.</td>
<td>Yes, unless encrypted and recipient unable to create own &quot;key&quot;</td>
</tr>
<tr>
<td>Misdirected e-mail of listing of drug seeking patients to an external group list</td>
<td>Yes</td>
</tr>
<tr>
<td>Papers containing PHI found on sidewalk outside [org] facility</td>
<td>Yes</td>
</tr>
<tr>
<td>Stolen/lost laptop containing unsecured PHI</td>
<td>Yes</td>
</tr>
<tr>
<td>Unencrypted PDA with patient-identifying wound photos lost</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*If "not required" is indicated, may still need to report based on the other risks (financial, reputational, etc.) and/or sensitivity of the information/situation at hand; document decision made & reasons for this decision
Sample Breach Notification Log

The organization shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. A record of the complete investigation of the potential breach as well as the risk assessment carried out to determine notification requirements should be created. The risk assessment and the record/incident report should be cross referenced so that should the Secretary of HHS require more information, it is easy to locate and provide.

Note: Reconfigure Width of Data Fields for Landscape Document or Spreadsheet

<table>
<thead>
<tr>
<th>Incident #</th>
<th>Date of Discovery</th>
<th>Date of Breach</th>
<th>Location</th>
<th>Brief Description of Breach*</th>
<th>Number Patients Involved</th>
<th>Notification Dates</th>
<th>Actions Taken</th>
<th>Resolution Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- A description of what happened, including 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, account number, etc.).
# Risk Assessment Analysis Tool

**Note:** For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule

<table>
<thead>
<tr>
<th>Q#</th>
<th>Question</th>
<th>Yes - Next Steps</th>
<th>No - Next Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Unsecured PHI</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Was the impermissible use/disclosure unsecured PHI (e.g., not rendered unusable, unreadable, indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary)?</td>
<td>Continue to next question</td>
<td>Notifications not required. Document decision.</td>
</tr>
<tr>
<td></td>
<td><strong>Minimum Necessary</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Was more than the minimum necessary for the purpose accessed, used or disclosed?</td>
<td>Continue to next question</td>
<td>May determine low risk and not provide notifications. Document decision.</td>
</tr>
<tr>
<td></td>
<td><strong>Was there a significant risk of harm to the individual as a result of the impermissible use or disclosure?</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Was it received and/or used by another entity governed by the HIPAA Privacy &amp; Security Rules or a Federal Agency obligated to comply with the Privacy Act of 1974 &amp; FISA of 2002?</td>
<td>May determine low risk and not provide notifications. Document decision.</td>
<td>Continue to next question</td>
</tr>
<tr>
<td>4</td>
<td>Were immediate steps taken to mitigate an impermissible use/disclosure (ex. Obtain the recipients’ assurances the information will not be further used/disclosed or will be destroyed)?</td>
<td>May determine low risk and not provide notifications. Document decision.</td>
<td>Continue to next question</td>
</tr>
<tr>
<td>5</td>
<td>Was the PHI returned prior to being accessed for an improper purpose (e.g., A laptop is lost/stolen, then recovered &amp; forensic analysis shows the PHI was not accessed, altered, transferred or otherwise compromised)?</td>
<td>May determine low risk and not provide notifications. Document decision. Note: don't delay notification based on a hope it will be recovered.</td>
<td>Continue to next question</td>
</tr>
<tr>
<td></td>
<td><strong>What type and amount of PHI was involved in the impermissible use or disclosure?</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Does it pose a significant risk of financial, reputational, or other harm?</td>
<td>Higher risk - should report</td>
<td>May determine low risk and not provide notifications. Document decision.</td>
</tr>
<tr>
<td></td>
<td>Question</td>
<td>Risk Level</td>
<td>Action</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Did the improper use/disclosure only include the name and the fact services were received?</td>
<td>May determine low risk and not provide notifications. Document decision.</td>
<td>Continue to next question</td>
</tr>
<tr>
<td>8</td>
<td>Did the improper use/disclosure include the name and type of services received, services were from a specialized facility (such as a substance abuse facility), or the information increases the risk of ID Theft (such as SS#, account#, mother's maiden name)?</td>
<td>High risk - should provide notifications</td>
<td>Continue to next question</td>
</tr>
<tr>
<td>9</td>
<td>Was a limited data set [164.514(e)] or de-identified data [164.514(b)] used or disclosed? Note: take into consideration the risk of re-identification [164.514(c)] (the higher the risk, the more likely notifications should be made).</td>
<td>Continued to next question</td>
<td>Continue to #11</td>
</tr>
<tr>
<td>10</td>
<td>Is the risk of re-identification so small that the improper use/disclosure poses no significant harm to any individuals (ex. Limited data set included zip codes that based on population features doesn't create a significant risk an individual can be identified)?</td>
<td>May determine low risk and not provide notifications. Document decision.</td>
<td>Continue to next question</td>
</tr>
</tbody>
</table>

**Specific Breach Definition Exclusions**

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
<th>Risk Level</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Was it an unintentional acquisition, access, or use by a workforce member acting under the organization's authority, made in good faith, within his/her scope of authority (workforce member was acting on the organization's behalf at the time), and didn't result in further use/disclosure (ex. billing employee receives an e-mail containing PHI about a patient mistakenly sent by a nurse (co-worker). The billing employee alerts the nurse of the misdirected e-mail &amp; deletes it)?</td>
<td>May determine low risk and not provide notifications. Document decision.</td>
<td>Continue to next question</td>
</tr>
<tr>
<td>12</td>
<td>Was access unrelated to the workforce member’s duties (ex. did a receptionist look through a patient's records to learn of their treatment)?</td>
<td>High risk - should provide notifications</td>
<td>Continue to next question</td>
</tr>
<tr>
<td>13</td>
<td>Was it an inadvertent disclosure by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same organization, or its OHCA, and the information was not further used or disclosed (ex. A workforce member who has the authority to use/disclose PHI in that organization/OHCA discloses PHI to another individual in that same organization/OHCA and the PHI is not further used/disclosed)?</td>
<td>May determine low risk and not provide notifications. Document decision.</td>
<td>Continue to next question</td>
</tr>
</tbody>
</table>

21 Updated 8/19/10.
22 Updated 8/19/10.
| 14 | Was a disclosure of PHI made, but there is a good faith belief than the unauthorized recipient would not have reasonably been able to retain it (Ex. EOBs were mistakenly sent to wrong individuals and were returned by the post office, unopened, as undeliverable)? | May determine low risk and not provide notifications. Document decision. | Continue to next question. Note: if the EOBs were not returned as undeliverable, these should be treated as breaches. |
| 15 | Was a disclosure of PHI made, but there is a good faith belief than the unauthorized recipient would not have reasonably been able to retain it (ex. A nurse mistakenly hands a patient discharge papers belonging to a different patient, but quickly realized the mistake and recovers the PHI from the patient, and the nurse reasonable concludes the patient could not have read or otherwise retained the information)? | May determine low risk and not provide notifications. Document decision. | Document findings. |

**Burden of Proof:** Required to document whether the impermissible use or disclosure compromises the security or privacy of the PHI (significant risk of financial, reputational, or other harm to the individual).