DRAFT
Template: Health Information Privacy and Security Breach Notification Letter

Health and Human Services Interim Final Rule for Breach Notification for Unsecured Protected Health Information, provided for in the American Recovery and Reinvestment Act of 2009 (ARRA), was implemented September 23, 2009. This rule serves to mitigate harm to a victim of an unprotected information breach whether or not the potential harm is economic. Covered entities are obligated to comply with these updated HIPAA privacy rule regulations as of September 23, 2009; though a five-month grace period delayed the imposition of noncompliance penalties until February 22, 2010.

While breach notification of an individual may be carried out through various methods, all applicable breaches in any medium require a notification letter with prescribed content. This article offers a template letter format for covered entities, with content customizable to an incident and to an organization. An organization may be one of the 44 states (along with the District of Columbia, Puerto Rico, and the Virgin Islands) currently further obligated to comply with differing state breach notification laws. They may be similarly obligated to balance other federal regulations with ARRA and state laws. This tool is intended to serve as a guide and does not seek to dictate content and format or disavow other content and format advice.

This federal rule[1] requires the breach message to be presented at an appropriate reading level and in clear language and syntax. To ensure the letter is adequate to be helpful, no length constraints are directed. However it should not include extraneous material detracting from the message.

The letter is approached in three stages:

1. Required elements must be addressed in a customized manner according to situational circumstances:
    - 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

2. Elements for customized inclusion if appropriate:
    A. Recommendations that the individual contact his or her credit card company and information about how to contact the credit bureaus and obtain credit monitoring services (if credit card information was breached)
    B. Information about steps the covered entity is taking to retrieve the breached information, such as filing a police report (if a suspected theft of unsecured protected health information occurred)
    C. Information about steps the covered entity is taking to improve security to prevent future similar breaches
    D. Information about sanctions the covered entity imposed on workforce members involved in the breach

3. Required or desired elements to be identified by the responsible healthcare organization according to specific state laws, applicable federal regulations, and organizational policy.

Italics are used in the template document to indicate variables—those areas needing an organization's substitution of specific facts, choices, options, and special considerations. Additional content may be further required or desired depending on setting, state, federal, and organization nuances specified in number three above.

Letterhead Recommended
(Includes organization's full name and address)

[Date]

[Victim or Representative Name]
[Address Line 1]
[Address Line 2]
[City, State Zip Code]

Re: Personal *[Health]* Information of *[Name of Victim]*

Dear [Addressee Name -- Victim or Representative]:

On *[date], [name of responsible healthcare organization]* became aware of a breach of *[your/loved one's*] personal health information. We *[have identified/estimate]* the date of information leakage to be *[date]*. *OR [The duration of information exposure was (include date range and time range)]*. OR [*We are unable to determine the date of the breach occurrence.]* We are notifying affected individuals in as timely a manner as possible so you can take swift personal action along with our organization's efforts to reduce or eliminate potential harm. *[It was necessary to delay notification because of the protected nature of the forensic investigation.]* Incident investigation *[is/is not]* complete at this time.[2]

The incident[3] involving protected health information was *[loss/theft/other] [state the circumstances]*. *[Examples: theft of a laptop containing files of 5,326 individuals from the trunk of a car* OR *exposure of personal health information on the (name of organization) Web site* OR *misplacement of five boxes, 250 paper medical records, during transit to a vendor destruction site]*. The unsecured information includes *[list the types of information involved: part/complete medical records dated between (state date range), full name, Social Security Number, date of birth, home address, account number, diagnosis, types of treatment information, disability code, name other information types]*.[4]

We recommend immediate steps be taken to protect *[yourself/your loved one]* from *[additional/potential]* information breach harm *[List fitting recommendations such as:*

- *Register a fraud alert with the three credit bureaus listed here; and order credit reports:*
  - *Experian: (888) 397-3742; www.experian.com; PO Box 9532, Allen, TX 75013*
  - *TransUnion: (800) 680-7289; www.transunion.com; Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790*
  - *Equifax: (800)525-6285; www.equifax.com; PO 740241, Atlanta, GA 30374-0241*
- *Monitor account statements, EOBs, and credit bureau reports closely*
- *Contact the Consumer Protection Agency [Sample Google search for appropriate state: "consumer protection agency Illinois"]*
- *(If the consumer has validation their information has been compromised) Notify law enforcement to assist the investigation: [Provide advice on how to file and provide contact information for local law enforcement, the state attorney general office, and the Federal Trade Commission]*

- *Access helpful Web links to learn additional information on consumer protection when personal information is compromised. [List Web links or provide own organization's Web site] [For example, include AHIMA's Medical Identity Theft Response Checklist for Consumers: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_039114.pdf]*

*[Name of responsible healthcare organization/**s**]*[5] *[has/have taken* OR *will soon take]* these steps to protect your, and others', personal information from further harm or similar circumstances: *[Choose from or customize these examples or add your own]:*

- *Initiated a forensics security investigation*
- *Filed a police report on [date]; Initiated a criminal investigation*
- *Sanctioned five employees/a physician by suspension/termination of employment/medical staff privileges*
- *Address operational or technology updates or changes triggered by the incident to improve confidentiality, such as strengthening technology safeguards or administrative policies and/procedures*
- *List steps a business associate is taking or investigation/cancellation of a business associate contract*
- *List any specific, relevant state law factors/directives*
- *Other*

State Law Customization Considerations—At appropriate points in the letter above, insert additional information required by state law such as:

- *Number of involved victims*
- *Potential level of threat to victims*
- *Possible future information security threats victims should be aware of*
- *The definition of PHI in your state*
- *What agencies were notified, such as state health department, state attorney general, and state police*

Furthermore, [name or responsible healthcare organization] is offering (you/name of individual) # years of free credit monitoring service. To take advantage of this offer, (give instructions to initiate the protection)].

[Name of responsible healthcare organization] sincerely apologizes for the inconvenience and concern this incident causes you. Your information privacy is very important to us and we will continue to do everything we can to correct this situation and fortify our operational protections for you and others.

You may contact us with questions and concerns in the following ways: *[by calling our Privacy Office at our toll free number (XXX) XXX-XXXX between the hours of X a.m. and X p.m., 24 hours or Monday to Friday; sending an e-mail message to xxxx@xxxx.org; addressing a letter to our postal address, Anywhere Hospital, 1234 Hospital Way, City, State].*

Sincerely,

[Name and title of an individual with knowledge of the incident]
[Contact information – may be the same as the contact information listed above]

Notes:

1. Organizations may be under additional presentation requirements with other federal laws such as Title VI of the Civil Rights Act of 1964; the Rehabilitation Act of 1973, Section 504; and the Americans with Disabilities Act of 1990
2. The urgency of the circumstances may require a notification letter be sent before the investigation is complete. A CE may determine a need to send a follow-up letter when more information is known.
3. The Interim Final Rule does not currently direct the provider to release the names of the individuals responsible for the breach.
4. HHS emphasizes that the exact or sensitive information breached should not be listed in the notification letter
5. A decision must be made whether to list one or both the contracting and contracted organizations in the information provided in the letter when a business associate is involved.

References:

- H.R.1 American Recovery and Reinvestment Act of 2009 (http://thomas.loc.gov)
- 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule (http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf)
- 13402(f) Notification in the Case of Breach, Content of Notification (http://thomas.loc.gov)
- Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule) (http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt)

Note: This template letter requires customization and is not intended for adoption as a substitute for a personalized breach notification letter with action steps appropriate to specific incident factors. Users are encouraged to adapt this sample letter as long as they in no way suggest their use or adaptation is endorsed by AHIMA. You do not need permission from AHIMA to adapt the letter for your use. Users may not use this template letter for commercial purposes.