Elements of a Breach Notification Letter

Save to myBoK

This month covered entities are subject to penalties for noncompliance with new federal privacy and security breach notification laws issued by the Department of Health and Human Services.

HHS issued an interim final rule titled "Breach Notification for Unsecured Protected Health Information" in August 2009. The rule, called for in the American Recovery and Reinvestment Act, serves to mitigate harm to victims of an unprotected information breach whether or not the potential harm is economic.

The rule took effect September 23, 2009, though a five-month grace period delayed the imposition of penalties for noncompliance until this month. Penalties begin February 22.

While breach notification may be carried out in various methods, all applicable breaches in any medium require a notification letter with prescribed content.

The Required Contents

The federal rule requires the breach message to be presented at an appropriate reading level and in clear language and syntax. The rule does not indicate how long a letter should be; however, it must include the following elements at minimum, and it should not include extraneous material that would detract from the message.

The letter is approached in three stages:

1. Required elements, which must be addressed in a customized manner according to the circumstances of the breach:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known
- A description of the types of unsecured protected health information that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, diagnosis, or disability code)
- Any steps the individual should take to protect themselves from potential harm resulting from the breach
- A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches
- Information on how individuals can contact the organization to ask questions or learn additional information, including a toll-free telephone number, an e-mail address, Web site, or postal address

2. Elements for customized inclusion, if appropriate:

- 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)
- 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)
- Information about steps the covered entity is taking to improve security to prevent future similar breaches
- Information about sanctions the covered entity imposed on workforce members involved in the breach

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

Customizable Letter Template

A breach notification letter template that may be adapted and customized by individual organizations is available to AHIMA members at www.ahima.org/arra. (See "Breach Notification Template Letter" under the heading "HITECH." Member ID and password are required to download file.)

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 disclosure 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 with 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]*

Other Laws May Apply

Currently 44 states, the District of Columbia, Puerto Rico, and the Virgin Islands have their own breach notification laws. Organizations thus may be further obligated to comply with differing state breach notification laws because the federal law does not preclude more stringent state requirements. Organizations may be similarly obligated to balance other federal regulations with ARRA and state laws.

Further, 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. It is essential

that covered entities be aware of all obligations for breach notification.

References

AHIMA. “Health Information Privacy and Security Breach Notification Letter.” Available online at www.ahima.org/arra.

Department of Health and Human Services. “Breach Notification for Unsecured Protected Health Information; Interim Final Rule.” *Federal Register* 74, no. 162 (Aug. 24, 2009). Available online at http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.

Article citation:
Hjort, Beth M.. "Elements of a Breach Notification Letter" *Journal of AHIMA* 81, no.2 (February 2010): 35.