



Please Print On Covered Entities (CE) Letterhead

Sample Notification Letter to Residents

Review and customize this letter based on your specific breach incident. Mandated content and timelines can be found in the Breach Notification for Unsecured Protected Health Information; Interim Final Rule, 164.404 and 164.408. This letter must be mailed first-class to the individual at their last known address or by electronic mail if the individual agrees to electronic notice.

[Date]

[Name here]

[Address 1 Here]

[Address 2 Here]

[City, State Zip Code]

Dear [Name of Resident]:

I am writing to you with important information about a recent [unauthorized disclosure/access/posting, etc.] of your personal information from [Name of CE or Business Associate (BA)]. We became aware of this event on [Insert Date] which occurred on or about [Insert Date].

Brief Description of Incident

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).

Steps We Have Taken

A brief description of what the CE or BA is doing to investigate the breach, to mitigate potential harm to individuals, and to protect against further breaches such as reporting to appropriate authorities, reviewing policies, audit and monitoring, re-education, employee disciplinary action...

We take the privacy and security of your protected health information very seriously. We have taken the following steps:

Steps You May Take

Any steps the individual should take to protect themselves from potential harm resulting from the breach such as notifying your health insurance company, changing your account numbers, notifying credit monitoring agencies...

We recommend that you:

For Additional Information Contact

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.

We regret that this [event]of protected health information has occurred and wish to assist you with any questions you may have. If you need additional information or wish to contact us with concerns, we are happy to speak with you. Please contact us at:

Optional Content

CE's may decide to offer credit monitoring services in addition to contact information for credit agency reporting.

To help ensure that this information is not used inappropriately, [Name of CE/ BA] 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; P.O. Box 740241, Atlanta, GA 30374-0241.

- **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013.
 - **TransUnion:** 1-800-680-7289; 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.

Closing Statement

While we are uncertain whether your personal information was actually obtained, we want to bring this situation to your attention. We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. [Name of CE/BA] apologizes for this situation and is taking appropriate measures to prevent a reoccurrence.

Sincerely,

[Insert Applicable Name/Contact Information]