Health Information Compliance Alert

Toolkit: Design Your Own HIPAA Breach Notification Letter with this Template

Tip: No matter the breach size, you must let patients know.

If a HIPAA breach occurs at your practice, you are bound by federal law covered under the HIPAA Breach Notification rule to alert any individual -patients, business associates, or employees - that the breach impacts. Moreover, for those that don't comply with the requirements or drag their feet on the notification process, the penalties can be steep.

"If you don't report the breach according to the rules, you are subject to the penalties for willful neglect of the rules," warns **Jim Sheldon-Dean**, Principal and Director of Compliance Services for Lewis Creek Systems, LLC, in Charlotte, Vermont.

Further, if the patient finds out about a breach and you didn't properly notify him, "he may file a complaint with HHS, at which point it will be too late to be in compliance," continues Sheldon-Dean.

Remember These Notification Guidelines

A timely and thorough response is expected by the HHS Office for Civil Rights (OCR) and is outlined in the HIPAA Breach Notification rule. "A covered entity must notify the secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach," the HHS notification guidance says.

Breaches that include fewer than 500 individuals:

- The covered entity must alert the HHS Secretary of the breach within 60 days of the calendar year in which the breach occurred.
- You must file the breach notification electronically, but you can submit the breach notifications on the same day - even if they occur on different days and concern separate issues.
- You must alert individuals impacted by the breach.

Breaches that include more than 500 individuals:

- You must file the breach notification electronically, and all information on the forms must be complete and comprehensive regarding the breach.
- You must notify the media of the breach.
- You must alert affected individuals to the loss of their protected health information (PHI).

Solution: Use this sample template as a guide when crafting your own HIPAA breach notification, but make sure you are using it as a guide only. If your practice isn't prepared to offer a full year of free credit monitoring, for instance, be sure to reword that part of the letter.

Sample HIPAA Breach Notification Letter

[Affected Individual's Name]
[Affected Individual's Address]
Dear [Affected Individual]:

This letter is part of [Provider's Name]'s commitment to patient privacy. Everyone at [Provider's Name] takes the issue of patient privacy very seriously, and it is important to [Provider's Name] that you are made fully aware of a potential

privacy issue.

[Provider's Name] has learned that your personal information, including name, address, _____, _____, and _____, might have been compromised. On [Date of Potential Breach Discovery], we discovered that [Description of Incident and Date of Potential Breach]. We reported the incident to the police because theft may have been involved (if applicable). However, we have not received any indication that any unauthorized individual accessed or used the information.

While we at [Provider's Name] are doing everything we can to protect your PHI, you can help protect your personal information by:

[Describe steps patient should take to protect themselves:]

[Provider's Name] is aware of how important your personal information is to you. If you choose, as an added security measure, we are offering one year of credit monitoring and reporting services at no cost to you [if applicable]. This service is performed through [Name of Vendor], an organization that watches for unusual credit activity and reports to you. [Name of Vendor] will also request that the three credit bureaus place a "Fraud Alert" on your credit report.

If you would like to receive this service free of charge for a year, please respond "yes" by checking _____ or "no" by checking _____.

We understand that this may pose an inconvenience to you. We sincerely apologize and regret that this situation has occurred. [Provider's Name] is committed to providing quality care, including protecting your personal information, and we want to assure you that we have policies and procedures to protect your privacy.

If you want to take advantage of the free credit monitoring service, or if you have any questions, please contact [Provider's Phone Number].

Sincerely,
[Name] Privacy Officer
[Provider's Company Letterhead]