Privacy Data Breach Notification To Affected Individual



Data breaches can happen even when you try diligently to prevent them. If your company experiences such a breach, you must perform an immediate assessment to determine the nature and extent of the breach, including the affected individuals and whether they're likely to experience what's known as real risk of significant harm (RROSH). Significant harm may include (but isn't limited to) bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property. If you do determine that the breach meets the RROSH threshold, you must notify affected individuals as soon as feasible after the breach occurs and provide them certain information.

Here's a template Breach Notification for notification of a breach compromising medical laboratory testing results that you can adapt for any scenario. **Caveat:** The template contains the basic information a company should include in a breach notification to an affected individual. However, your company may be subject to laws or parties to contracts that impose special or additional breach reporting requirements. So, be sure to talk to a lawyer when adapting the template for your own use.

NOTICE OF PERSONAL DATA BREACH

ABC COMPANY

Re: Notice of Privacy Breach Affecting Your Personal Records

Dear [*name of affected individual*]:

Please be advised that on [*date breach discovered*], ABC Company ("Company") employees discovered that a data security breach occurred that may affect the privacy of your protected health information. The purpose of this letter is to offer our apologies and to describe the breach, its potential impact on you and the steps you can take to minimize the harm to your priva

Brief Description of Breach: The breach occurred on [*date of breach*] when [*explain what happened*] [*example: a night-time custodial worker employed by one of our independent contractors gained unauthorized access to a database containing private laboratory test records on you and other Company clients*.]

Personal Information Involved: As a result, of this unauthorized and unexpected intrusion, the worker was able to gain access to the medical records and protected health information of you and other patients, including [*list the type of information involved in the breach, e.g., names, Social Insurance Numbers, street addresses, dates of birth, test results, and diagnoses*.]

Company Response: On [*date*], [*number of*] days after learning of the breach, Company reported the incident to the police and began an internal investigation. Company also plans to implement the following measures in response to the investigation's findings [*describe measures taken to limit the potential privacy impact of the breach and ensure that it never happens again*] [*example: to limit the risk of financial damage, we are offering you and other clients affected by the breach one year's worth of credit monitoring and reporting at no cost to you. Please notify us at the contact number below if you want to accept this offer by [date]*].

Suggested Protective Measures: So far, Company has obtained no evidence indicating that the worker has actually used or shared the patient personal health information to which he gained unauthorized access. However, we are offering you protection in the form of the free credit monitoring service noted above. We also suggest that you call the toll-free numbers of one of the major credit bureaus to place a fraud alert on your credit report:

- Equifax Canada: 1-800-465-7166 or 1-866-828-5961
- TransUnion Canada: 1-800-663-9980

You need only contact one of the agencies. Once a fraud alert is placed with one agency, the other one will receive notification and place its own alerts. The credit bureau will also explain how to obtain a free copy of your credit report that you can examine for signs of fraud. You should also continue to monitor your credit report going forward to ensure no fraud or identity theft takes place.

Contact Information: If you have any questions or would like further information regarding the breach, please call the Company's special toll-free number [*phone number*] during normal business hours. Company has also established a section on its web site [*URL*] where it will post updated information and links to other sites offering information to help you protect yourself against fraud and identity theft.

Closing Apology: In closing, the Company would like to apologize to you for the inconvenience and personal stress you may suffer as a result of this breach. Please be assured that we are keenly aware of our obligation to safeguard the privacy and security of the personal health information that our clients entrust to us and that we have adopted strict policies and technological solutions to meet that obligation. The breach, we believe, represents an aberration, one that we are determined to learn from and prevent from ever happening again.

Sincerely yours,

[Privacy Officer/IT Manager]