TEVORA™

Breach Notification Guide

For HIPAA, FTC, GDPR, and CCPA

Chad Stanger

Derek Glausser

Edward Martinez

Matthew Cheung

May 31, 2022

Table of Contents

Glossary of Terms

- **CCPA:** California Consumer Privacy Act
- **ENISA:** European Union Agency for Cybersecurity
- **EU:** European Union
- **FTC:** Federal Trade Commission
- **GDPR:** General Data Protection Regulation
- **HIPAA:** Health Insurance Portability and Accountability Act
- **HITRUST:** Health Information Trust Alliance
- **PHI:** Protected Health Information
- **PHR:** Personal Health Record
- **SSN:** Social Security Number

Breach Notification Rules

In the healthcare sector, the main goal of HIPAA is to protect patient data from being disclosed without patient consent. But suppose patient data is breached, what actions should you take? Who do you need to report to, and what information do you need to include? In this paper, we will discuss the breach notification rules for responding to a breach for HIPAA, FTC, GDPR, and CCPA, respectively. If your organization encounters or suspects a breach, Tevora offers many services such as Incident Response, Compliance Consulting, Disaster Recovery, and Remediation Support.

HIPAA

Under the HIPAA Breach Notification Rule, business associates and covered entities will provide notifications whenever there is a breach of unsecured protected health information (PHI). Examples of PHI include name, social security numbers, and email address. We will discuss HIPAA's definition of a breach and cover the notification requirements. Additionally, we provide a template for writing a breach notification letter in the appendices.

Setting for HIPAA

We discuss the setting where HIPAA Breach Notification rule applies. The United States Department of Health and Human Services (HHS) defines a breach as an impermissible use or disclosure that compromises the security and privacy of PHI. Unauthorized disclosure is considered a breach unless the covered entity or business associate conducts a risk assessment showing a low probability that PHI has been compromised based on at least the following factors:

1. Nature and extent of the PHI
2. The unauthorized individual
3. Whether the PHI was viewed or received
4. the extent to which the risk was mitigated

There are three exceptions for where an unauthorized disclosure is no longer classified as a breach.

1. Unintentional use of PHI of a worker under the authority that was done under good faith
2. Accidental disclosure from a person authorized to access PHI from one business associate/covered entity to another.
3. Covered entities/business associates have valid reasons to believe the unauthorized individual/individuals could not attain access to the PHI.

Breach Notifications for HIPAA

There are three types of notifications: notifications to Secretary, notification to individuals affected, and notifications to covered entities.

Covered entities are required to provide the notification to the Secretary. This is done online through the web form on the HHS website given here: Form for Secretary. If the number of individuals affected is above 500, the online form must be submitted within 60 days of the discovery of the breach. If the number of individuals affected is below 500, the online form must be submitted no later than 60 days before the end of the calendar year that the breach was discovered. If the number of individuals cannot be determined, the covered entities must provide an estimate. Any additional information acquired after submitting the form can be submitted online as well by checking the box indicating the addendum to the original report. A new report does not need to be filed.

Covered entities are required to provide notification to individuals. The notification requirements depend on two cases:

- More than 10 individuals have insufficient or outdated contact information
- Fewer than 10 individuals have insufficient or outdated contact information

In the first case, the substitute individual notice must either be a notice on the home page of the covered entities' website or a print or broadcast of the situation nearby where the individual lives. Furthermore, the covered entities must provide a toll-free phone number for at least 90 days that affected individuals can call if they wish to learn more about the breach. In the second case, the substitute individual notice includes some alternative form of written notice, telephone call, or other forms of contact.

Business associates must notify covered entities no later than 60 days of the discovery of the breach. The business associates should include logs of the breach and information such as the affected individuals' names, contact information, type of data breached, and other relevant information if possible.

FTC

Many web-based companies that deal with personal health records (PHR) are not covered by HIPAA. Therefore, the Federal Trade Commission (FTC) enacted the Breach Notification Rule for vendors of PHR, PHR-related entities, or third service party providers. A PHR-related entity is anyone who works with the vendor of PHR such as offering services to the vendor, accessing PHR from the vendor, or sending PHR from the vendor. Examples of PHR-related entities are web-based services that offer web applications for health information. Third-party entities are businesses that offer services involving PHR to vendors or PHR-related entities.

Setting for FTC

We define the setting where FTC applies. For the FTC, vendors, PHR-related entities, or third-party businesses fall into the Breach Notification Rule if there is an unauthorized acquisition of PHR-identifiable information that is unsecure and, in a PHR. An unauthorized acquisition is any information maintained or used without the permission of the affected individual. The FTC defines unsecure PHR-identifiable information as information that is not encrypted or destroyed.

Breach Notifications for FTC

The notifications can be categorized into two cases:

- When over 500 individuals are affected
- When fewer than 500 individuals are affected

In the first case, the affected individuals, FTC, and media need to be notified. For notifying affected individuals, the rule states that notification must happen within 60 days and without unreasonable delays. For example, if the breach information is discovered and gathered on the first day, reporting the breach to individuals 60 days after the discovery is an unreasonable delay. The FTC must be notified within 10 days using an online form provided in Form for FTC. If there are over 500 individuals affected within a state, the media outlets near where the individuals reside must be notified within 60 days of the discovery of the breach. The notification to the media does not count as notification to the affected individual. In the second case, the affected individuals and the FTC must be notified. The notifications for affected individuals remain the same, but businesses have until 60 days following the end of the calendar year to notify the FTC.

The organization must determine whether individuals prefer email or first-class mail. If customers choose email as the default method for communication, they must be notified that first-class mail is an alternative. New customers choosing to use email must be notified breach notifications will come in the form of an email. The notification should include the following:

1. Description of the breach incident
2. The PHR information involved in the breach
3. Suggestions on protective actions affected individuals can take
4. Steps for investigation and remediation
5. Contact information

Exception to the Rule

If you are a HIPAA business associate dealing with only PHI of HIPAA covered entities, you are not obligated to perform the breach notifications as specified by the FTC. If you are a HIPAA business associate but also handle PHR (e.g., health records collected from an app), you may be obligated to perform breach notifications for both HIPAA and FTC.

GDPR

When personal data is breached for individuals from the EU, the EU privacy laws come into effect. The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy. In the case of a breach, the GDPR considers four parties: the controllers, processors, affected individuals, and the supervisory authority of the EU country of the affected individuals. Data controllers determine the purpose and means for which the PHI is processed. Data processors process the PHI on behalf of the data controller.

Setting for GDPR

As outlined in GDPR, the definition of a personal data breach is, "breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed." [6] Personal data is any data related to the identified person such as name and ID.

Breach Notification Rule for GDPR

In the case of a personal data breach, the supervisory authorities of the EU and the affected individuals must be notified.

The controller must notify the supervisory authority of the EU country for the affected individual no later than 72 hours after the discovery of the breach. For example, if a personal data breach involves individuals in Spain, England, and France, then notifications must be sent to the supervisory authority of Spain, the supervisory authority of England, and the supervisory authority of France. The processor must notify the controller without delay about the breach. The notification to the EU authorities will include the following:

1. Description of personal data breach incident number of affected individuals and data records
2. Name and contact information of the affected individuals to the data protection officer
3. Likely consequences of the breach
4. Actions taken to remediate the situation

If there is a high risk to the rights of the individual, the controller must notify the affected individuals as well. European Union Agency for Cybersecurity (ENISA) recommends using their assessment for the severity of personal data breaches to determine whether the risk is high. There are three cases where notifications to individuals are not necessary:

1. Controllers have implemented measures in such a way that the data is unintelligible to unauthorized individuals (e.g., encryption).
2. There is no high risk to the rights and freedoms of the individual.
3. Communication will require a disproportionate effort.

However, the controller has the choice to not immediately notify the individual, they may notify the authorities first. If the EU supervisor authorities determine that no notification to the individual is required (i.e., they determine one of the three points above are satisfied), no action is needed for notifying the affected individuals.

CCPA

The California Consumer Privacy Act (CCPA) gives consumers who are residents in California control over their personal information. California residents may ask businesses to facilitate certain rights afforded to them under CCPA, including:

- The right to know about the personal information a business collects about them and how it is used and shared
- The right to delete personal information collected from them
- The right to opt-out of the sale of their personal information
- The right to non-discrimination for exercising rights

Businesses subject to the CCPA are given new obligations to facilitate these new rights. Businesses are expected to initiate the data subject's right to be notified. Businesses fulfil this obligation by providing a "notice at collection", a privacy policy. This notice must be provided at or before the point a business collects a data subject's personal information. The categories and purposes of this collection must be included in the notice.

Additionally, businesses must create reasonably accessible means for a data subject to exercise their consumer rights.

Setting for CCPA

We define the settings we will work with for the CCPA. It is important to differentiate how personal information is defined by California as opposed to the CCPA. California defines personal information as the individual's name along with one of the following:

1. SSN
2. Driver's license or another government-issued identification number (e.g., Passport card)
3. Account number or credit or debit card number
4. Medical or health insurance information
5. Biometric data (e.g., Fingerprints)
6. Information from license plate registration
7. Username or email address with password

For the CCPA, personal information is defined to be "information that identifies, relates to, describes, is capable to be associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." [1]

From an enterprise perspective, the CCPA applies to for-profit businesses that meet at least one of the following:

1. Gross annual revenue of $25 million
2. Buy, sell, or receive personal information of over 50,000 California residents, households, or devices
3. Receive 50% or more of their annual revenue from California residents

The CCPA does not apply to non-profit businesses and government agencies.

Breach Notification for the CCPA

California requires a business to notify any California resident whose information is believed to have been acquired by an unauthorized individual. Since the notification requirements lie outside the bounds of CCPA, we will not cover them in this whitepaper. When the business notifies the California residents of the unauthorized acquisition, the CCPA provides provisions for actions the residents can take.

While personal information is defined by the CCPA, the scope of personal information is restricted if a consumer wishes to sue the business when there is a breach. Consumers may only sue businesses if the information is not encrypted and unredacted. Furthermore, the personal information must be the individual's name along with one of the following:

1. SSN
2. Driver's license or another government-issued identification number
3. Financial account number, credit card number, or debit card number
4. Medical or health insurance information
5. Biometric data

If all conditions above are satisfied, consumers may sue businesses for monetary damages up to $750 per incident. As for suing for statutory damages (i.e., violations to the CCPA), the consumer must write to the businesses on what parts of the CCPA were violated. The business has 30 days to give you a report stating that the violation is fixed, and no future violations will occur. If the violation is not fixed or future violations do occur, consumers will be allowed to sue. For any other damages or violations to the CCPA, consumers must file a complaint to the Office of the Attorney General given here: Notification to General. The Attorney General will be responsible for deciding whether to file against the business based on investigations.

Appendix A - HIPAA Breach Letter Template

This is an example of a template letter that business associates may use to send to covered entities if fewer than 500 individuals are affected.

Date
Customer (covered entity)
Title
Address Line 1
Address Line 2

Dear Customer (covered entity),

This letter serves as a notification that there has been a breach within our company. The breach occurred on [Date of Occurrence] and was discovered on [Date of Discovery].

[Include paragraph here on the breach incident and type of information that was breached. Examples include patient name, social security information, date of birth, address, etc.]

[Include a few sentences here on what you have done to investigate the breach and steps you will take to prevent future breaches.]

We need you to do the following:

1. Notify the Secretary of breaches of unsecured protected health information. This can be done online through Breach Reporting. We will provide for you from our end the information of the breach through the Excel sheet given. Since less than 500 individuals were affected, this must be done no later than 60 days at the end of the calendar year.
2. Notify the individuals affected through first-class mail or email if the individual is receiving notices electronically. If more than 10 or more individuals have outdated information or insufficient contact information, a substitute notice must be provided. Substitute notice can be a notice on the home page of your website for at least 90 days or through media that broadcast near where the individual lives. Furthermore, you must provide a toll-free phone number that those individuals can call to learn if their information was breached. If under 10 individuals have outdated information or insufficient contact information, a substitute notice of written form or telephone call is appropriate. Please do this within 60 days of [Date of Discovery].

We deeply apologize for this incident, and we assure you that we are taking the appropriate actions to remedy the situation.

Sincerely,

Authorized Contact Name / Signature

Appendix B - GDPR Breach Letter Template

Below, we include an example of a letter from the controller to the authority if the controller has not notified the affected individuals is given below.

[Date]
Title
Address Line 1
Address Line 2

Dear Supervisor authority of [insert EU country here],

This letter serves as a notification that there has been a breach within our company. The breach occurred on [Date of Occurrence] and was discovered on [Date of Discovery].

[Include paragraph here on breach incident and the type of information that was breached].

[Include a few sentences here on what you have done to investigate the breach, consequences, and steps you will take to prevent future breaches]

Notifications to affected individuals have not been made. [Give reasons why you fall into one of the 3 items listed above]. If you deem notification to data subjects necessary, we will do so, but we will refrain from notifying individuals unless you view the incident as high risk.

We deeply apologize for this incident, and we assure you that we are taking the appropriate actions to remedy the situation.

Sincerely,

Authorized Contact Name / Signature

Appendix C - References

1. Bonta, R. *California Consumer Privacy Act*. State of Department of Justice. CCPA 1

2. Bonta, R. *Consumer Complaint Against a Business/Company*. State of Department of Justice. CCPA 2

3. Clara, M. and Slawomir G. (2013, December 20). *Recommendations for a methodology of assessment of severity of personal data breaches*. Enisa. ENISA Severity Assessment

4. Federal Trade Commission (2009, August). *Health Breach Notification Rule*. Federal Trade Commission Protecting America's Customers FTC Notification

5. Federal Trade Commission (2010, April). *Complying With the FTC's Health Breach Notification Rule*. Federal Trade Commission Protecting America's Customers FTC Report Description

6. Intersoft Consulting. *Chapter 4 Controller and Processor*. General Data Protection Regulation GDPR Chapter 4

7. Office for Civil Rights (2013, July 26). *Breach Notification Rule*. Health Information Privacy. HIPAA Breach

8. Office for Civil Rights (2015, January 5). *Submitting Notice of a Breach to the Secretary*. Health Information Privacy. HIPAA Breach 2

9. Office for Civil Rights. *Notice to Secretary of HSS Breach of Unsecured Protected Health Information*. U.S. Department of Health and Human Services. HIPAA Breach 3

10. RadarFirst. (2020, March 24). *CCPA vs. California Breach Notification Law: What's the Difference?*. RadarFirst Blog CCPA 3

Author Profiles

Chad Stanger, Information Security Consultant

Primary Role

As an information security consultant for Tevora’s ISO and Healthcare Security Compliance team, Chad’s primary role is to support and lead ISO and healthcare information security assessments. In addition, Chad helps organizations identify policy, process, and implementation gaps. Chad performs remediation support alongside these organizations, so they can become compliant with ISO, HIPAA and HITRUST certification requirements

Notable Accomplishments

Chad began his experience in security assessments, compliance, and risk management in 2019. Chad has performed multiple types of security assessments including ISO, HIPAA and HITRUST gap assessments and risk assessments.

Certification and Training

ISO/IEC 27001 Lead Auditor
HITRUST Certified CSF Practitioner (CCSFP)
Certified HITRUST Quality Professional (CHQP)

Tenure

Chad has been with Tevora since June 2019.

Derek Glausser, Information Security Associate

Primary Role

Derek Glausser is an Information Security Associate responsible for contributing to various projects within the Privacy team and ISO 27001 practice at Tevora.

Notable Accomplishments

Derek possesses a bachelor’s degree from the University of Pittsburgh, Pennsylvania, specializing in Economics and Political Science. He leverages his education to have a robust understanding of legal frameworks and regulation standards related to privacy and security.

Certification and Training

Derek completed a fellowship at Carnegie Mellon University focused on Information Systems and Information Security. Derek is currently working towards a CIPP/E certification.

Tenure

Derek has been with Tevora since May 2021

Edward Martinez, Information Security Analyst

Primary Role

Edward Martinez is an Information Security Analyst at Tevora, an information security management consulting firm out in Southern California. Since 2020, Edward has worked in the Healthcare practice, specializing in HIPAA and HITRUST, aiding clients to achieve certification.

Notable Accomplishments

Prior to starting Tevora, Edward studied mathematics with an emphasis on number theory and cryptography, attaining a Master of Science in Mathematics from UC Irvine.

He has presented on various topics including agent-based modeling and classical, elliptic curve, quantum, and post-quantum cryptography. He was a member of a cryptography group at UCI which reviewed several pre-prints and currently provides technical reviews for books on cryptography.

He has helped Tevora build various tools to aid in assessments and help build the practice to ensure client satisfaction. Chad holds a Bachelor of Science (B.S.) degree with a dual emphasis in management information systems and operations management.

Certification and Training

Edward holds the following certifications: HITRUST CCSFP and a Cryptology Certificate from ASU.

Tenure

Edward has been with Tevora since January 2020.

Matthew Cheung, Developing Consultant

Primary Role

Matthew is part of the Consultant Development Program at Tevora and is responsible for helping with assessments from HITRUST and HIPAA.

Notable Accomplishments

Matthew has constructed a Sage code for point counting on singular hypersurfaces. The code generalizes to smooth surfaces such as elliptic curve. This has applications to elliptic curve cryptography in the TLS which is known to be safer to quantum computer attacks.

Certification and Training

Matthew has earned a master’s degree in mathematics and will receive his PhD degree in mathematics in June.

Tenure

Matthew has been with Tevora since April 2022.

About Tevora

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and serve institutional and government clients.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that can fully implement whatever it recommends, Tevora works with the industry's top vendors yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication have established us as a reliable partner CTOs CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information, please visit www.tevora.com.

Our team of consultants is ready to discuss your specific challenges and identify the best solutions.

TEVORA™

Go forward. We’ve got your back.

Email us: sales@tevora.com

Call us: 833.292.1609