DATASHEET

Radar® Privacy

The FTC Health Breach Notification Rule in Radar® Privacy

Simplified FTC compliance for personal health apps and devices

The FTC's 2009 Health Breach Notification Rule requires that vendors of personal health records (PHR), PHR-related entities, and third-party service providers, including health apps and connected devices, provide notification of security breaches involving unsecured PHR identifiable health information. Penalties for noncompliance are significant—and increase annually with inflation.

The FTC's Health Breach Notification Rule

In 2009, the FTC issued the Health Breath Notification Rule, which requires vendors of personal health records, PHR-related entities, and third-party service providers not covered by HIPAA to notify consumers, the FTC, and, in certain cases, the media of any breaches involving unsecured PHI.

In 2021, the FTC clarified that the Health Breach Notification Rule **applies to developers of health apps and connected devices**. This was partly due to the growing use of wearable fitness devices and related apps. The FTC has also **increased enforcement efforts, resulting in significant fines and penalties.**

The FTC has offered clarification that health apps and connected apps are subject to the Health Breach Notification Rule.

Critical Updates to the Rule:

The amended Health Breach Notification Rule includes, but is not limited to, the following revisions, which were published in the Federal Register on May 30, 2024, and will take effect 60 days after publication on July 29, 2024:

- Additional clarification that **the rule applies to health apps** and similar technologies not covered by HIPAA
- Clarification that **a "breach of security" under the rule includes unauthorized disclosure**, as well as a breach that occurs as a result of a data security breach
- **A revised definition of "PHR-related entity"** to make clear that only entities that access or send unsecured PHR identifiable health information to a personal health record qualify as PHR-related entities
- **An expansion of the required content provided in the notice to consumers** including the names of any third parties who might have acquired any unsecured PHR identifiable health information and at least two methods of contact for affected individuals to obtain additional information
- Modification to the timeline requirements for FTC notification in events involving **500 or more affected individuals**

Entities Covered Under the Health Breach Notification Rule

You are covered by the Breach Notification Rule if you are not a HIPAA-covered entity, and you are a:

Vendor of personal health records. Your business is a vendor of personal health records if it offers or maintains a personal health record. A personal health record is defined by the FTC as an electronic record of "PHR identifiable

health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."

PHR-related entity. Your business is a PHR-related entity if it interacts with a vendor of personal health records either by offering products or services through the vendor's website—even if the site is covered by HIPAA—or by accessing information *in* or sending information *to* a personal health record.

Third-party service provider. Your business is a third-party service provider if you access, maintain, retain, modify, record, store, destroy, or otherwise use or disclose unsecured PHR identifiable health information in service to a vendor of personal health records or PHR-related entity.

Who Must be Notified Under the Health Breach Notification Rule

Affected individuals. Notification must be sent without unreasonable delay and in **no case later than 60 calendar days** after the discovery of a breach of security.

The FTC. The notification deadline is determined by the number of individuals affected by the breach. If 500 or more individuals are affected, notification is required in 10 business days. Events involving less than 500 individuals can be submitted in a log no later than 60 days after the end of the calendar year.

The media. When **500 or more residents** of a particular state, the District of Columbia, or a U.S. territory or possession are affected by a breach, the covered entity must notify prominent media outlets serving the relevant locale. Notification must be sent without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.

Clients, customers, and partners. Companies acting as **third-party service providers** to vendors of personal health records or PHR-related entities must identify for their client each person whose information may be involved in the breach, so that their clients can in turn notify affected individuals, the FTC, and the media as required. Notification must be sent without unreasonable delay and in no case later than 60 calendar days after discovery of a breach of security.

***If the breach involves the information of 500 people or more**, organizations covered by the Health Breach Notification Rule must notify the FTC **as soon as possible and no later than 10 business days** after discovering the breach.*

Automated FTC Notification Obligation Intelligence with Radar® Privacy

The FTC has increased its enforcement of the Health Breach Notification Rule. This can challenge privacy professionals who are still using manual tools to assess incidents. The consequences of non-compliance can be costly to both an organization's reputation and budget

Automation to Simplify FTC Compliance

The FTC Health Breach Notification Rule is unique in that it: offers a broad definition of individually identifiable information, it doesn't explicitly define data elements considered personal information, and that it does not provide a harm standard as a condition of notification in the event of a breach.

The **FTC module in Radar® Privacy** is uniquely configured to comply with the Health Breach Notification Rule. Patented assessment automation and intelligent notification guidance ensure consistency and decrease time to resolution, so your organization can meet even the strictest FTC notification timelines.

Schedule a Demo >