



## FAQ: Health Breach Notification Rule Proposed Rule

Updated: June 2023

The Federal Trade Commission (FTC) [released](#) a proposed rule that seeks to amend the Health Breach Notification Rule on June 9, 2023. This rule proposes amendments that would clarify the Health Breach Notification Rule's applicability to health applications and other similar technologies. The FTC seeks to better protect the privacy and security of personal health data amid the rise in health apps and other direct-to-consumer technologies, the increased collection of health data from consumers, and the risk of companies inappropriately using or disclosing sensitive data. The FTC released a [press release](#) on the proposed rule. **Public comments are due August 8, 2023.**

### Key Provisions of the Proposed Rule:

- Revise the definition of “personal health record (PHR) identifiable health information” and newly define the terms “health care provider” and “health care services or supplies” to clarify that the scope of the Health Breach Notification Rule covers developers of health applications
- Amend the definition of “breach of security” to clarify that a breach of security includes unauthorized acquisitions of data that occur from a data breach or unauthorized disclosure
- Revise the definition of “PHR related entity” to clarify that the Health Breach Notification Rule covers entities that offer products and services through the websites and any online services, including mobile applications, of vendors of personal health records
  - The rule also proposes to revise this definition to clarify that only entities that access or send unsecured PHR identifiable *health* information to a personal health record (rather than entities that access or send *any* information to a personal health record) qualify as PHR related entities
- Revise the definition of “personal health record” to reflect an electronic record of PHR identifiable information on an individual that has the technical capacity to draw information from multiple sources and that is managed, shared, and controlled by or primarily for the individual
  - Under this proposed revision, a product is a personal health record if it can draw any information from multiple sources, even if it only draws health information from one source
- Modernize the method of notice to authorize the use of email and other electronic means of providing clear and effective notice of a breach to consumers
- Expand the content of the notice to require that consumers who's unsecured PHR identifiable information has been breached receive additional important information (i.e., the potential for harm from the breach and protections the notifying entity is making available to affected consumers)
- Improve the rule's readability by clarifying cross-references and adding statutory citations, consolidating notice and timing requirements, and specifying penalties for non-compliance

If you have questions, please contact the AHIMA Advocacy and Policy team at [advocacy@ahima.org](mailto:advocacy@ahima.org).