

HEALTH LAW

Update

NEWS FOR THE CLIENTS AND FRIENDS OF BASS, BERRY & SIMS PLC

The FTC's Proposed Notification Rule for Breach of Personal Health Record Information: More Consumer Protections for an Internet-Based World

May 5, 2009

On April 16, 2009, the Federal Trade Commission ("FTC") issued notice of a proposed rule that would require certain entities that offer personal health records ("PHR") to notify consumers when the security of their electronic health information is breached.¹ A PHR, which has a slightly different meaning than "electronic health record," is a record that end-user consumers of healthcare can access directly online to manage their health information. Healthcare consumers, rather than healthcare providers, maintain PHRs. The FTC is seeking comments to its proposed PHR rule, which are due by June 1, 2009.

The FTC issued the proposed rule in order to comply with the American Recovery and Reinvestment Act of 2009 ("ARRA"), also known as the economic stimulus bill, which was signed into law on February 17, 2009. ARRA acknowledges that new types of internet-based entities collect and handle personal health information, allowing consumers to track and manage their health information online. ARRA requires the FTC to work with the Department of Health and Human Services ("HHS") to conduct a study and report on potential privacy, security and breach notification requirements for PHR vendors, PHR-related entities, and third-party service providers. The report must be completed by February 2010.

In the interim, ARRA mandates that the FTC promulgate temporary regulations requiring affected entities to notify affected consumers if the security of their PHR information is breached. These regulations will apply to entities that are *not* subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). In the FTC's notice of proposed rulemaking, the FTC makes clear that ARRA also requires HHS to promulgate interim final regulations applicable to HIPAA-covered entities and their business associates.²

¹ 74 Fed. Reg. 17914 (April 20, 2009).

² Pursuant to ARRA, HHS issued guidance to HIPAA-covered entities on April 17 regarding "technologies and methodologies to secure health information and prevent harm by rendering health information unusable, unreadable, or indecipherable to unauthorized individuals."

Affected Entities

The proposed rule, if finalized as written, will apply to PHR vendors, other PHR-related entities, and those vendors' and entities' third-party service providers.³ Therefore, the proposed rule will apply to entities outside the FTC's normal jurisdiction, including nonprofit organizations that offer PHRs. Other examples of PHR-related entities include companies that advertise dietary supplements online, entities that offer web-based applications to help consumers manage medications, and websites offering online personalized health checklists. Under the proposed rule, third-party service providers (which is not a defined term under ARRA) include entities that provide services such as billing or data storage to PHR-related entities or vendors of PHR.

Breach of Security

Consistent with ARRA, the proposed rule defines "breach of security" as the acquisition of unsecured PHR identifiable health information of an individual in a PHR without the individual's authorization.⁴ The key to the triggering of a notification requirement is whether the data has actually been acquired, not whether the entity experienced unauthorized access to its systems records or information. The FTC makes clear that the term "acquisition" means that the information is not only available to unauthorized persons but in fact has been obtained by the unauthorized persons. The FTC also makes clear that the entity that experienced the breach is in the best position to determine whether an actual unauthorized acquisition has taken place, though the proposed rule creates a presumption that unauthorized persons have acquired information if they have access to it, thus triggering the obligation to provide breach notification. The presumption can be rebutted with reliable evidence showing that the information either was not or could not reasonably have been acquired.

"PHR identifiable health information"

The proposed rule defines "PHR identifiable health information," to include not only health information but also information relating to past, present, or future payment,⁵ which therefore includes databases containing names and credit card information. The FTC also makes clear that the mere information that an individual has an account with a PHR vendor or PHR-related entity regarding a particular health condition constitutes "PHR identifiable health information."

Notice Requirements

The proposed rule requires PHR vendors and PHR-related entities to notify U.S. citizens and residents upon discovery of a breach of security and also to notify the FTC.⁶ Upon discovering a security breach, third-party service providers are required to provide notification to the appropriate vendors and entities so that the vendor or entity can in turn provide its customers with a breach notice. Breach notifications must be made to affected individuals and the media "without unreasonable delay" after the entity or vendor knows or reasonably should have known

³ If finalized, the requirement will be found at 16 C.F.R. § 318.3.

⁴ If finalized, the definition will be found at 16 C.F.R. § 318.2(a).

⁵ If finalized, the definition will be found at 16 C.F.R. § 318.2(e).

⁶ If finalized, the requirement will be found at 16 C.F.R. § 318.3.

of the breach and in no case later than 60 calendar days after discovery of the breach.⁷ If the breach involves the unsecured PHR identifiable health information of 500 or more individuals, notification to the FTC must be made no later than five business days after discovery.

Notification may be provided (a) by written notice sent by first-class mail to the individual's last known address or by email if the individual has expressly affirmed consent to so receive notices, (b) by telephone in the case of imminent misuse of unsecured PHR identifiable health information, or (c) in certain cases where the individual has affirmatively indicated preference for either first-class mail or email, but the affected vendor or entity believes such information to be outdated, by another form of communication.⁸ Further, if ten or more individuals cannot be reached by the methods listed above, the vendor or entity shall provide notice through a conspicuous posting on the home page of its website, which must remain in place for six months, or by major print or broadcast media.

The proposed rule specifies that the content of the notice must include: (a) a brief description of how the breach occurred, including the date of the breach and the date of the discovery; (b) a description of the types of unsecured PHR identifiable health information that were involved in the breach; (c) steps affected consumers should take to protect themselves from potential harm; (d) a brief description of what the entity that suffered the breach is doing to investigate, mitigate losses, and protect against future breaches; and (e) contact procedures for affected individuals to ask questions or get additional information.⁹

The FTC makes clear in the proposed rule that violations of the breach notification requirement will be treated as an unfair or deceptive act or practice.¹⁰ If you have any questions about the proposed rule or other matters discussed in this *Health Law Update*, please do not hesitate to contact one of the attorneys in our Healthcare Practice Group listed on the following page.

⁷ If finalized, the requirement will be found at 16 C.F.R. § 318.4.

⁸ If finalized, the requirement will be found at 16 C.F.R. § 318.5.

⁹ If finalized, the requirement will be found at 16 C.F.R. § 318.6.

¹⁰ If finalized, this regulation will be found at 16 C.F.R. § 318.7.

Bass, Berry & Sims Healthcare Attorneys

H. Stanford Adams, Jr.
(615) 742-7775
sadams@bassberry.com

Kevin L. Alonso
(615) 742-7913
kalonso@bassberry.com

H. Lee Barfield, II
(615) 742-6202
lbarfield@bassberry.com

Philip F. Berg
(615) 742-7908
pberg@bassberry.com

Krista Thornton Cooper
(615) 742-7734
kt Thornton@bassberry.com

Mary Beth Fortugno
(615) 742-7739
mfortugno@bassberry.com

Nesrin E. Garan
(615) 742-7903
ngaran@bassberry.com

Pooneh Ghiassi
(615) 742-7782
pghiassi@bassberry.com

Anna Grizzle
(615) 742-7732
agrizzle@bassberry.com

Elisa E. Harris
(615) 742-6553
eharris@bassberry.com

Angela Humphreys
(615) 742-7852
ahumphreys@bassberry.com

Clevonne M. Jacobs
(615) 742-7769
vjacobs@bassberry.com

J. James Jenkins, Jr.
(615) 742-6236
jjenkins@bassberry.com

Seth A. Killingbeck
(615) 742-7707
skillingbeck@bassberry.com

David King
(615) 742-7890
dking@bassberry.com

Claire F. Miley
(615) 742-7847
cmiley@bassberry.com

T. Scott Noonan, Co-Chair
(615) 742-6273
tnoonan@bassberry.com

Brenda N. Phillips
(615) 742-6237
bnphillips@bassberry.com

Shannon Pinkston
(615) 742-7727
spinkston@bassberry.com

Cynthia Y. Reisz
(615) 742-6283
creisz@bassberry.com

Brian D. Roark
(615) 742-7753
broark@bassberry.com

Scott B. Shanker
(901) 543-5932
sshanker@bassberry.com

Catherine J.B. Sloan
(615) 742-7789
csloan@bassberry.com

Danielle M. Sloane
(615) 742-7763
dsloane@bassberry.com

Leigh Walton, Co-Chair
(615) 742-6201
lwalton@bassberry.com

Elizabeth S. Warren
(615) 742-7719
ewarren@bassberry.com

Douglas M. Wolford
(615) 742-7917
dwolford@bassberry.com

The materials contained herein have been abridged from the statutory sources and should not be construed or relied upon for legal advice. Readers are urged to consult legal counsel concerning particular situations and specific legal questions.

To ensure compliance with requirements imposed by the IRS, we inform you that this message is not intended to be used, and cannot be used, by the addressee or any other person for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code.

315 Deaderick Street • Suite 2700 • Nashville, TN 37238-3001 • (615) 742-6200
The Tower at Peabody Place • 100 Peabody Place, Suite 900 • Memphis, TN 38103-3672 • (901) 543-5900
1700 Riverview Tower • 900 S. Gay Street • Knoxville, TN 37902 • (865) 521-6200