PROSKAUER ROSE LLP

A Moment of Privacy

A newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose

MARCH 2009

Edited by
Kristen J. Mathews and
Tanya L. Forsheit

Welcome to "A Moment of Privacy," a newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose LLP.

"A Moment of Privacy" addresses one legal development each month in the area of privacy and data security law. We answer the questions our clients are asking, in a way that we hope gives practical information to our readers. If you send us your question, you may find your answer in an upcoming newsletter.

And now for this month's question:

Q: I have been waiting for resolution of the question: Do the Federal Trade Commission's Identity Theft Red Flag Rules apply to health care providers? With the May 1st compliance deadline looming, my company needs to know.

A: The answer seems to depend on whom you ask. The Federal Trade Commission ("FTC") and the American Medical Association ("AMA") have been in discussions regarding this point for the last several months.* Most recently, in a February 4th letter to the AMA, the FTC reiterated its earlier position stating that the Red Flag Rules apply to health care providers who regularly defer payment for medical services. In a February 23rd letter responding to the FTC, the AMA "strongly objected" to the FTC's interpretation and alleged that the FTC failed to comply with the Administrative Procedures Act ("APA") since it did not explain in advance its rules' application to health care providers nor provide the public with notice and opportunity to comment. In summary, the AMA asked the FTC to either withdraw its interpretation or conduct a new rulemaking procedure that complies with the APA.

The Identity Theft Red Flag Rules require covered entities to implement a program to detect and respond appropriately to signs of identity theft. For a health care provider, this would mean, as an example, detecting situations in which a patient may be attempting to obtain medical services using another person's identity and medical insurance policy.

Since the FTC's position on this issue has been firm, unless and until the AMA obtains a stay on enforcement of the rules, medical care providers should gear up for compliance. According to the FTC, for many providers of medical care, compliance may not be too

burdensome since their programs need only be scaled to the level of risk of identity theft faced by their patients. So if the risk is low, the identity theft program can be streamlined commensurate with such risk.

As examples, a health care provider could implement a program that includes, among other things:

- Checking patients' photo IDs when medical services are sought
- Responding appropriately when notified by a consumer or law enforcement agency that the consumer's identity has been misused
- Isolating suspect medical records from the victim's medical records
- Suspending collection efforts against the medical identity theft victim relating to services provided to the unauthorized individual

Depending on the size and complexity of the provider, a more robust program may be necessary.**

*See http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm for the FTC's September '08 article on the applicability of the Red Flag Rules to health care providers.

**See http://www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf for The World Privacy Forum's suggestions for health care providers addressing the Red Flag Rules. See http://www.hhs.gov/healthit/documents/MedIdTheftReport011509.pdf for a January '09 report commissioned by the U.S. Dep't of Health and Human Services' Office of the National Coordinator for Health Information Technology regarding medical identity theft, including suggestions to prevent medical identity theft and actions to take in the event that medical identity theft is suspected.

Have a question? E-mail Kristen J. Mathews at kmathews@proskauer.com.

Privacy and Data Security Practice

Our Privacy and Data Security Practice is an outgrowth of our Internet, intellectual property, technology media & communications, labor and employment, health law, First Amendment, international law and litigation practices. Indicative of our experience and reputation in this relatively new field of law is the fact that the venerable Practising Law Institute (PLI) asked our Firm to create its first-ever treatise on the subject of privacy and data security law, called "Proskauer on Privacy," which was published in late 2006.

Privacy and Data Security Practice Group Partners:

Tanya L. Forsheit
310.284.4508 – tforsheit@proskauer.com

Grégoire Goussu
33.1.53.05.60.11 – ggoussu@proskauer.com

Kristen J. Mathews
212.969.3265 – kmathews@proskauer.com

Jeffrey D. Neuburger
212.969.3075 – jneuburger@proskauer.com