



Law Office:  
428 McLaws Cr Suite 200  
Williamsburg VA 23185

Voice 757.259.9200  
Fax 757.259.9201  
Toll free 877.635.5388 (Mellette)

Mailing Address:  
P.O. Box 6133  
Williamsburg VA 23188

## **CLIENT ADVISORY:**

### **Federal Trade Commission Issues Guidance to Healthcare Providers on Medical Identity Theft**

In January 2011, the Federal Trade Commission (“FTC”) issued guidance to healthcare providers on medical identity through a list of Frequently Asked Questions. The FAQs explain the problem of medical identity theft and list ways to minimize the risk and help patients who are victims. The guidance is available at <http://business.ftc.gov/documents/bus75-medical-identity-theft-faq-health-care-health-plan>. The FTC notes that while identity theft is typically associated with financial transactions, it also occurs in the context of medical care when someone uses another person’s personal information to obtain medical treatment or medication. As the FTC explains, victims of medical identity theft may receive bills for services they did not receive, be contacted by a debt collector regarding medical debts they do not owe, or be denied insurance because their medical records show a condition they do not have.

Of particular interest to healthcare providers is the FTC’s guidance on the proper response to medical identity theft. Once a healthcare provider learns that a patient may be a victim of medical identity theft, the FTC suggests that the provider conduct an investigation. Such an investigation, depending on the circumstances, may require a review of medical records and verification of the identity of the person receiving services. In addition, healthcare providers, to the extent they report debts to credit reporting agencies, may have obligations under the Fair Credit Reporting Act. If an internal investigation reveals that the healthcare provider improperly used or shared protected health information, the provider should then determine if the breach falls under the HIPAA Breach Notification Rule or any applicable Virginia law.

Healthcare providers should exercise care in helping patients correct any medical, billing, or financial records that may have been affected by medical identity theft. Like all patients, the affected person should be given a copy of the HIPAA-covered provider’s Notice of Privacy Practices. The provider should also advise the victim to take advantage of their rights under HIPAA – including the right to request copies of their medical records, the right to have their medical and billing records amended or corrected, the right to an accounting of disclosures, and the right to file a complaint with the U.S. Department of Health and Human Services’ Office for Civil Rights (“OCR”). Exercising these rights will help a patient affected by medical identity theft identify the extent of the damage and make necessary corrections. Healthcare providers may also encourage patients to notify their health plan of any suspected identity theft, contact the FTC and law enforcement, and look for signs of other misuses of their personal information.

Medical identity theft can profoundly affect a victim's financial situation and medical care. Failure to follow required data security practices in compliance with the HIPAA Privacy and Security Rules can also expose healthcare providers to liability in the form of Civil Money Penalties ("CMP") and other liabilities. In February 2011, OCR imposed a CMP of \$4.3 million for violations of the HIPAA Privacy Rule. Other healthcare organizations have made hefty payments to settle privacy complaints brought by OCR. It is essential that all healthcare providers – regardless of the size of organization – periodically and routinely review their privacy and security practices compliance. Comprehensive compliance programs include elements such as employee training, careful drafting and implementation of policies and procedures, internal audits, and prompt attention to incidents.

If our firm can be of assistance in explaining the FTC guidance or reviewing your organization's compliance with the HIPAA Privacy and Security Rules, please let Peter Mellette, Harrison Gibbs, or Nathan Mortier know.