Unlike financial identity theft, which targets a victim’s financial health, medical identity theft threatens a victim’s very existence. The unauthorized access of a victim’s medical record not only grants the thief access to the victim’s personal identifying and financial information, but also allows that thief to fraudulently use the victim’s identity to obtain medical goods and services. The access and use of a victim’s medical record results in a co-mingling of medical histories and a contamination of the victim’s medical record with false diagnoses, an inaccurate medical history, and improper drug prescriptions. The erroneous medical record not only puts the victim at risk, but also has a negative impact on the quality of care delivered by health care providers, exposes payors to potential improper billing or overbilling, and/or subjects health organizations to privacy breaches.

Medical identity theft is 50 times more lucrative for a thief than stealing a Social Security number. In 2013, medical identity theft increased by 19 percent, affecting nearly 1.84 million adult individuals. According to the World Privacy Foundation, the cost of such theft is estimated to total more than $30 billion. With the lucrative nature of medical identity theft and the Affordable Care Act dramatically increasing the pace at which medical health information is digitized, individuals, providers, payors, and health information organizations are increasingly more vulnerable to medical identity theft attacks.

The California Attorney General’s Recommendations

In response to an increase in medical identity theft and electronic medical record vulnerabilities, California Attorney General Kamala D. Harris recently released a guide from the Privacy Enforcement and Protection Unit of the California Department of Justice entitled: “Medical Identity Theft: Recommendations for the Age of Electronic Medical Records.” In this guide, the attorney general classifies medical identity theft as a “quality-of-care issue that directly impacts the core mission of the health care industry,” and holds the entities in that industry responsible for preventing, detecting, and mitigating the effects of medical identity theft.

This guide is not a list of regulations, mandates or legal opinions, but rather, a list of “best practices” for health care providers, payors, health information organizations and policy makers. Its classification as “best practices” should not dissuade these entities from taking the recommendations seriously. A failure to follow and ultimately implement these recommendations could prove detrimental to any health care provider, payor, or health information organization that has the misfortune of sustaining a medical identity theft.

Recommendations for Health Care Providers

Health care providers should create: (1) a medical identity theft response team; and (2) a medical identity theft response plan.

The Response Team

The depth of the team will depend upon the size of the organization. For large organizations, the response team should consist of the privacy officer, as well as members from administration, information technology, compliance, records, billing, security, human resources, each clinical department, patient registration, and the providers themselves. For smaller organizations, the response team should consist of a member from the front-office staff, office management, billing, information technology, and the providers themselves.
The Response Plan

The plan should include policies and procedures that address the prevention, detection, and mitigation of medical identity theft.

Prevention. The written policies and procedures should address the screening, training, and access controls of staff, including temporary hires and volunteers, to any medical information, and the protocol for verifying a patient’s identity upon presenting for medical care services.

**PePPER Point:** Do not forget to include business associates in the screening, training, and/or access control policies and procedures. Additionally, remember that it is against the law to delay or fail to treat a patient requiring emergency care even if that patient’s identity cannot be verified. Make a note of it in the record and then revisit at a non-emergent, appropriate time.

Detection. The written policies and procedures should identify discrepancies occurring at patient registration, billing and records management, and during the delivery of medical services that give rise to additional review and/or further investigation. Additionally, the policies and procedures should outline the investigative process, including the response to any patient complaints, the method to educate staff and patients about errors and fraud in the medical records, and the use of technology.

Mitigation. The written policies and procedures should establish the steps necessary to correct the actual medical record, and any other record affected by the medical identity theft.

**RECOMMENDATIONS FOR PAYORS**

Similar to health care providers, payers should also create a medical identity response team and establish a medical identity response plan that includes policies and procedures on prevention, detection, and mitigation.

Prevention. The written policies and procedures should focus on establishing reasonable and appropriate data security and privacy standards and safeguards, and educating the fraud investigation team on current medical identity theft trends.

Detection. The written policies and procedures should effectively incorporate and use the Explanation of Benefits statements, claims submission process, and fraud detection software.

Mitigation. The written policies and procedures should focus on resolving the fraudulent claim investigation in favor of limiting “the damage to consumers and support their efforts to clear problems related to their credit and pursuit of identity theft claims.”

**PePPER Point:** Here, the Attorney General’s recommendation focuses heavily on a payer’s responsibility to mitigate a consumer’s damages. A payer must ensure that its drafted policies do not favor the consumer to the detriment of itself.

**RECOMMENDATIONS FOR HEALTH INFORMATION ORGANIZATIONS**

While there is no universal definition for health information organizations, the California Attorney General defines this type of organization as one that “manages and oversees health information exchange functions.” Health information organizations are classified as business associates of the providers who use them. Common examples of health information organizations are electronic medical record vendors and health care clearinghouses. Since health information organizations are relatively new, and are growing rapidly, it is recommended, and expected, that these entities will build technology infrastructures that can assist in the prevention, detection and mitigation of medical identity theft.

**PePPER Point:** Health information organizations have a real opportunity to lead in the technical capabilities of preventing, detecting, and mitigating medical identity theft. Such an opportunity could prove extremely lucrative if executed correctly with the guidance of knowledgeable legal counsel.

**ENDNOTES**

1 According to Kirk Herath, Nationwide Chief Privacy Officer, “A stolen medical identity has a $50 street value—whereas a stolen Social Security number, on the other hand, only sells for $1.” *Claims Journal,* “Study: Few Aware of Medical Identity Theft Risk,” June 14, 2012.


4 Medical Identity Theft: Recommendations for the Age of Electronic Medical Records, pg. 1.

5 Medical Identity Theft: Recommendations for the Age of Electronic Medical Records, pg. 15.

6 Medical Identity Theft: Recommendations for the Age of Electronic Medical Records, pg. 3.