

# Medical Identity Theft: Highlights from the World Privacy Forum Report

## The Problem

WPF estimates that there could be as many as a quarter to a half million people who have been victims of this crime. FBI director Louis Freeh: "We have seen cocaine distributors switch from drug dealing to health care fraud schemes. The reason - the risks of being caught and imprisoned are less. Drug dealers who are committing health care fraud know that they likely will face only minor punishments because law enforcement is not yet equipped with the laws needed to effectively attack this problem."

Victims do not have clear pathways for recourse and recovery. The Fair Credit Reporting Act allows for greater recourse for victims of financial identity theft than the HIPAA health privacy rule provides for victims of medical identity theft. For example, victims do not have the legal right to demand correction of their medical information that was not created by the provider or insurer currently maintaining or using the information. This circularity can make it impossible for a medical identity theft victim to erase false entries from a medical or insurance record. This is true even when false entries were put in the record during the commission of a crime, such as health care fraud or medical identity theft. Victims of medical identity theft may receive the wrong medical treatment, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage. They may fail physical exams for employment due to the presence of diseases in their health record that do not belong to them. It is nightmarish that patients' medical records may include information about individuals who have stolen their identities for the purposes of using the victims' insurance or for dodging medical bills. However, evidence exists that this is already occurring.

## Case Studies

- A Boston area psychiatrist made false entries in charts of individuals who were not his patients. He gave individuals diagnoses of drug addiction and abuse, severe depression and numerous psychiatric sessions which they did not actually have, then used their personal information to submit false bills to insurance. The victims, after learning of the crime, had difficulties getting the false information removed from their medical files. One woman told an investigator that she "is concerned about obtaining future health insurance coverage ... because her husband is self-employed."
- Another non-patient of the same Boston psychiatrist discovered that his medical record had been falsified to include numerous psychiatric sessions that did not occur and false diagnoses of severe depression. He discovered the false diagnoses after he had applied for employment.
- One medical identity theft victim from Florida went for medical treatment and says she found that her medical files had been altered. She said that she discovered that an imposter had caused false entries on her file, including changes to her blood type.
- An Ohio woman, while working at a dental office, accessed protected patient information and used the information to phone in prescriptions to area pharmacies. According to the Office of Inspector General, Health and Human Service, she "called in prescriptions in her name as well as the names of Medicaid recipients."
- In another case, a Missouri identity thief used multiple victims' information to establish false drivers' licenses in their names. The thief entered a regional health center, acquired the health record of the victim she was impersonating at the time, and intentionally altered the records in order to obtain a prescription in the victim's name.
- A Pennsylvania man discovered that an imposter used his identity at five different hospitals to receive more than \$100,000 worth of medical treatment. At each hospital, the imposter created medical histories in the victim's name.
- Victims in Southern California were given medical tests by non-physicians and had false diagnoses inserted into their medical files by a sophisticated, organized network of medical imaging companies. The individuals, according to an indictment, actively recruited Medicare beneficiaries with the promise of free transportation, food, and medical care. The perpetrators, posing as doctors and health professionals, obtained the victim's personal information and photocopied the victim's Medicare cards. The operation raked in \$909,000 using victims' personal and insurance information.

## Policy Recommendations

The World Privacy Forum, as part of its ongoing in-depth research into medical identity theft issues and responses, has outlined 8 best-practice responses to the crime by the health care sector.

## National level procedures

There needs to be a national level set of procedures to standardize how providers and insurers should handle medical identity theft. The procedures should come from a consensus process that includes health information management professionals, patient representatives, consumer groups, insurers, privacy groups, and others. The standards need to address how to help victims recover from this crime.

There needs to be uniform but appropriately flexible answers to these questions:

- What do we do when a patient claims fraud is in their files?
- What do we do when a patient says the bills are for services did not receive?
- What do we do for patients and other impacted victims when we uncover a fraudulent operation?
- When we have a real case of medical identity theft, how can we work with patients to fix the records and limit future damages?
- What do we do when a provider has altered the patient records?
- How do we handle police reports and requests for investigation from victims?

### **Red flag alerts**

Red flag alerts in the financial context make financial institutions affirmatively react to the potential presence of fraud in order to protect consumers and themselves. Financial fraud red flag alerts have applicability to medical identity theft. In the medical identity theft context, a red flag alert would be placed in a victim's health care records to alert providers and insurers of potential fraudulent activity. The health care sector needs to create specific red flag guidelines for use in the medical identity theft context.

### **John or Jane Doe file extraction**

Health information managers will be familiar with this concept already. If fraud can be substantiated, the victim's file is purged of all information that was entered as a result of the fraud. Sometimes, this may be part of the file, in some cases the entire file may belong to the thief. If the thief is unknown, the fraudulent information is completely removed from the victim's file and held separately so there is no danger of mis-treatment due to factual error in the file. That separate file is the Jane or John Doe file. The victim's file and the extracted file are then cross referenced, allowing for a retraceable data trail for any audits.

### **Dedicated, trained personnel available**

Dedicated personnel trained to respond to this crime should be available at each facility. Small providers can have dedicated regional personnel to help. It is in the providers' or insurers' best interest to resolve this crime, and it is in the victims' best interest to be able to actually talk to a person about what has happened. There needs to be a designated person trained in the complexities of medical identity theft on hand to help both the victim and the institution.

### **Focus on the right approach: Insider, not outsider**

The preponderance of medical identity theft occurs through insider methods that are extremely difficult for providers to detect, even after the fact. Even when internal file browser controls and other controls are in place, unless there are safeguards with extensive checks, then bad actors on the inside of institutions can commit this crime on a grand scale. For example, in the Cleveland Clinic/ Machado case, there were existing controls on downloads of files. The criminal still was able to exceed her download limit regularly, and she sold in excess of 1,100 patient files. Many institutions have been focusing on checking patient IDs as the primary solution to medical identity theft. While checking patient IDs will help with the one-to-two person and familial types of medical identity theft, the research does not support that this is where the bulk of the crime is. There is significant variability between providers and situations, it is therefore crucial to accurately assess and focus on all aspects of where the crime is occurring. Checking patient IDs will not stop insiders, and this needs to be taken into careful consideration by stakeholders.

### **Risk assessments specifically for medical identity theft**

Most health care institutions already have risk assessments in place. The risk assessments need to be expanded to include medical identity theft scenarios. The assessment should include outsider threats, but should also have a strong focus on the insider threat scenario as well.

### **Training materials and education for the health care sector**

Many individuals and institutions working in the health care sector are not yet aware of medical identity theft. Health care sector leaders need to begin health care sector-focused education focused on increasing awareness of the crime, its operations, and how it impacts victims. Ideally, an education plan would be able to also discuss a national set of standards for dealing with the aftermath of medical identity theft with the purpose of helping victims.

### **Education for patients and victims**

Providers and other stakeholders in the health care sector need to begin patient and victim education regarding medical identity theft. The education should focus on increasing:

- Awareness of the crime
- Awareness of the benefits of requesting a *full* copy of the health care files from *all* providers proactively
- Awareness of the need to guard insurance and Medicare/ Medicaid card numbers as carefully as social security numbers
- Awareness of the need to pro-actively request an annual listing of all benefits paid by insurers