Raising Awareness of Medical Identity Theft: For Consumers, Prevention Starts with Guarding, Monitoring Health Information

by Laurie A. Rinehart-Thompson, JD, RHIA, CHP

Financial identity theft has become ubiquitous in our global society. Its consequences are familiar, and fear of its repercussions has created a widespread reliance on credit bureaus for protection. According to the Federal Trade Commission, 8.3 million Americans were reportedly affected by financial identity theft in 2005.[1]

Medical identity theft—often viewed as more sinister because of its combined financial impact and its potentially devastating effect on an individual's health status—has more recently emerged in the public's awareness.

What Is Medical Identity Theft?

Medical identity theft is a subset of identity theft, which involves the assumption of another's identity without that individual's consent.[2] The World Privacy Forum identifies two means of perpetrating medical identity theft.

First is the use of a person's name and sometimes other identifiers such as Social Security number, without the knowledge or consent of the victim, to obtain medical services or goods. Second is the use of a person's identity to obtain money by falsifying claims for medical services. In conjunction with this falsification, and of utmost concern to health information professionals and healthcare consumers alike, is the falsification of health records to support those claims.

Typically excluded from medical identity theft are situations where patient information is inappropriately changed but the identity of the patient is not assumed or abused by another. In such cases, the patient was negatively affected medically but not financially.

Likewise, the use of a patient's financial information to purchase goods or services that are not medical in nature does not constitute medical identity theft because the patient was negatively affected financially but not medically.[3]

To qualify as medical identity theft, both the patient's financial and medical information must be affected. Medical identity theft, not unlike financial identity theft, includes the use of existing accounts (e.g., incurring charges in the victim's name on an existent account) or new accounts (e.g., obtaining benefits using the victim's name and the perpetrator's photograph).[4] From 1992 to early 2006, the number of medical identity theft complaints filed with the Federal Trade Commission totaled approximately 19,400.[5]

Medical identity theft risks are typically associated with the theft of financial information such as credit cards and other account numbers for medical treatment purposes. However, the potential for harm goes much deeper.

What makes medical identity theft so potentially devastating is the fact that incorrect information—often reflecting the perpetrator's physical or mental characteristics—may be entered into a victim's health record as part of the crime. This exposes the victim to improper and potentially life-threatening treatment if critical medical conditions, procedures, medications, and allergies are either omitted from the record or wrongfully included. Additionally, life insurance or health insurance may be denied based on medical conditions the victim never had.[6]

Medical identity thieves are commonly individuals who are close to the victim and who may have the advantage of relatively easy access to the victim's information. These individuals include family members and friends.

However, perpetrators may also be amateurs who are not closely connected to the victim or professionals working independently or as part of a larger, organized network.[7] Medical identity theft has frequently been associated with healthcare professionals.[8]

A New Risk: Personal Health Records

The US healthcare system is increasingly advocating patient-centered healthcare and consumer convenience in light of a society that is increasingly mobile. As a result, personal health records (PHRs) are emerging as a way for healthcare consumers to manage and share their health information. However, depending on the manner in which healthcare consumers maintain their PHRs, the privacy of that information—both medical and financial—can be placed at risk.

First, the creation of a PHR involves the duplication of information housed in a new location, whether verbatim or as a summary, from primary sources such as hospitals, physician offices, and other providers.[9] Additionally, the portability of PHRs creates avenues for potential breaches as documents can be lost or misplaced. Portable documents include those maintained on media such as paper, disks, and USB drives.

Finally, there are PHRs that may be maintained by someone other than the healthcare consumer. These PHRs may be exposed to disclosures of which patients are unaware.

Gaps in HIPAA Protections

Implemented in 2003, the HIPAA privacy rule sought to provide healthcare consumers with long-awaited privacy protections and rights to their health information. However, with respect to medical identity theft, there are areas where HIPAA protections and rights may not extend. One exception is commercial PHR vendors.

Well known companies such as Microsoft and Google have announced services that allow healthcare consumers to store their health information in online repositories.[10] These commercial vendors offer the convenience of storing and maintaining PHRs that can be easily accessed from multiple locations. However, they do not meet the HIPAA covered entity definition of healthcare providers, health plans, or healthcare clearinghouses.

Healthcare consumers who possess a vague familiarity with HIPAA but lack a solid understanding of the law may broadly associate health information with HIPAA protections and thereby adopt a false sense of security. It is important that professionals responsible for safeguarding the health information of others take an active role to prevent such an incorrect association.

The HIPAA privacy rule provides consumers with the right to access their health information, the right to request an amendment when they believe information in the record is erroneous and, although quite limited, the right to an accounting of where their health information has been disclosed. However, after a perpetrator of medical identity theft has inserted erroneous information into the health record—often his or her own—a covered entity may refuse to grant these rights to the victim.

Some covered entities have taken a cautious approach to this situation by denying victims their rights under HIPAA and stating that the health record may no longer be accessed, amended, or its dissemination tracked by the victim because it contains protected health information that belongs to someone else. Although this interpretation is technically correct, it creates a vicious cycle for the victim, who watches a criminal's HIPAA rights supersede his or her own and is prevented from accessing, correcting, and tracking his or her financial and health information.

Other covered entities have taken a different approach. The privacy rule permits the disclosure of personal health information without patient authorization for payment purposes, which includes activities to obtain reimbursement. These activities include determining eligibility or coverage and reviewing healthcare services for medical necessity and justification of charges.[11] Covered entities favoring disclosure to the medical identity theft victim grant access as a disclosure for payment purposes to determine whether services were actually provided to the victim and should be billed accordingly.

What Consumers Can Do to Protect Themselves

The steps that consumers have become accustomed to in protecting themselves against financial identity theft translate well into medical identity theft prevention. Consumers must be diligent about monitoring their health information. The AHIMA e-HIM work group on medical identity theft recommends that healthcare consumers take the following measures:

- Share health and financial information only with trusted individuals, including providers
- Monitor benefits paid by their health insurers
- Contact the insurer about charges for care not rendered (even if there is no out-of-pocket cost to the consumer)
- Maintain copies of health records for comparison
- Check personal credit history for medical liens
- Safeguard all health insurance information including insurance cards, explanations of benefits, and correspondence
- Refuse to provide insurance information to solicitors, including those who entice healthcare consumers through offers of "free" medical services in exchange for personal and insurance information[12]

Although the medical identity theft victim does not fit neatly into a single profile, vulnerable victims include the elderly and individuals with developmental or intellectual disabilities. These individuals or those assisting them, as well as individuals responsible for newborns, other minors, and the affairs of deceased persons, must take special care to safeguard personal and medical information.[13]

Once medical identity theft has occurred, the victim should work with the organization where the medical identity theft occurred to stop future dissemination of erroneous information, correct it, and determine where it has been sent so appropriate retractions and corrections can be made. If the organization is a HIPAA covered entity that does not allow the victim to mitigate the damage through access, amendment, and an accounting of disclosures, a complaint may be filed with the Office for Civil Rights in the Department of Health and Human Services.

Other government entities that may provide assistance to victims of medical identity theft include the Federal Trade Commission, the Social Security Administration if misuse of a Social Security number is suspected, the attorney general of the state where the crime occurred, consumer protection departments (if they exist) of state departments of insurance, and local police departments. Fraud alerts should be filed with the victim's insurers, providers, and credit bureaus.[14]

Although medical identity theft can and does exist in paper environments, it operates and proliferates most easily in digital settings. As the face of health information changes, healthcare consumers must take it upon themselves to safeguard and monitor their health information with the same degree of diligence that they protect their financial information.

Resources for Consumers and HIM Professionals

AHIMA offers practice guidance on preventing medical identity theft within organizations and assisting consumers who have been victims of theft. The following materials are available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

Medical Identity Theft Response Checklist for Consumers

Consumers may follow this printable checklist for proactive guidance and quick action when confronted with medical identity theft. This single sheet is a Web extra to the practice brief "Mitigating Medical Identity Theft" (see below).

Mitigating Medical Identity Theft

This practice brief explores medical identity theft, its ramifications, and how HIM professionals and others can work together to prevent, investigate, and mitigate the damages it causes. First published in the *Journal of AHIMA* 79, no. 7 (July 2008).

Ensuring Security of High-Risk Information in EHRs

This practice brief identifies health information that may require a higher degree of security and recommends EHR system features that can help provide sufficient safeguards. First published in the *Journal of AHIMA* 79, no. 9 (Sept. 2008).

Notes

1. Andrews, Michelle. "Medical Identity Theft Turns Patients into Victims." *U.S. News and World Report*. February 29, 2008. Available online at www.usnews.com.
2. Dixon, Pam. "Medical Identity Theft: The Information Crime That Can Kill You." World Privacy Forum. May 3, 2006. Available online at www.worldprivacyforum.org/medicalidentitytheft.html.
3. Ibid.
4. Nichols, Cindy, ed. Medical Identity Theft. Chicago, IL: AHIMA, 2008.
5. Dixon, Pam. "Medical Identity Theft: The Information Crime That Can Kill You."
6. Ibid.
7. Nichols, Cindy, ed. Medical Identity Theft.
8. Dixon, Pam. "Medical Identity Theft: The Information Crime That Can Kill You."
9. Gellman, Robert. "Personal Health Records: Why Many PHRs Threaten Privacy." World Privacy Forum. 2008. Available online at www.worldprivacyforum.org/personal_health_records.html.
10. Andrews, Michelle. "Medical Identity Theft Turns Patients into Victims."
11. HIPAA, Public Law 104-191, 45 CFR §160.501.
12. AHIMA e-HIM Work Group on Medical Identity Theft. "Mitigating Medical Identity Theft." *Journal of AHIMA* 79, no. 7 (July 2008): 63–69.
13. Ibid.
14. Ibid.

Laurie A. Rinehart-Thompson (laurie.rinehart-thompson@osumc.edu) is an assistant professor of clinical allied medicine in the School of Allied Medical Professions at The Ohio State University in Columbus, OH.

Article citation:
Rinehart-Thompson, Laurie A.. "Raising Awareness of Medical Identity Theft: For Consumers, Prevention Starts with Guarding, Monitoring Health Information" *Journal of AHIMA* 79, no.10 (October 2008): 74-75;81.