Identity Theft and Fraud--the Impact on HIM Operations

Save to myBoK

This practice brief has been retired. It is made available for historical purposes only.

Identity theft and fraud are the fastest growing crimes today. Healthcare organizations are particularly vulnerable to identity theft due to the wealth of patient personal, demographic, and financial information that is collected, transmitted, and maintained in the course of operations. Healthcare employees with legitimate access to protected health information (PHI) may gather information for later misuse. Credit cards and identification may be stolen while patients are being treated in healthcare facilities. Individuals posing as investigators may contact patients or providers asking for information that allows them to impersonate the patient or provider.

Preventing identity theft poses many challenges for HIM professionals, including:

- Ensuring preventive safeguards are in place to protect the privacy and security of patient PHI
- Balancing patient privacy protections with disclosing identity theft events to victims, law enforcement officials, and federal agencies
- Identifying resources to assist healthcare organizations, providers, and patients who are victims of identity theft

Understanding Identity Theft and Fraud

Passed in 1998, the Identity Theft and Assumption Deterrence Act made identity theft a federal crime. The act defines identity theft as when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law." Penalties include up to 15 years imprisonment and a maximum fine of $250,000. The act also established the Federal Trade Commission (FTC) to act as a clearinghouse for complaints, referrals, and resources for victims of identity theft.

Identity theft and fraud refer to all crimes in which someone wrongfully obtains and uses another person's personal data (e.g., name, address, Social Security number, bank or credit card number), typically for economic gain. Thieves may use the information to:

- Make unauthorized withdrawals from financial accounts
- Use existing credit card accounts or open new ones
- Open other types of accounts (e.g., cell phone, utility)
- Take out loans
- Submit false insurance claims
- Assume another person's identity to obtain health benefits

In a healthcare environment, identity thieves may obtain information by:

- Accessing information under the pretext of a legitimate need and then diverting the information for criminal purposes
- Hacking into computerized patient information
- "Dumpster diving," or collecting information from the organization's trash or recyclables
- Stealing wallets, purses, or mail from patients, visitors, or staff

Healthcare organizations must ensure safeguards are in place to prevent identity theft as well as guidance for responding to identity theft incidents. Organizations should also help victims by ensuring appropriate contact and involvement with local law enforcement and other regulating agencies.

Practical Preventive Guidance

HIM professionals and healthcare organizations can take the following measures to help prevent identity theft:

1. Ensure appropriate background checks of employees and business associates who may have access to the organization's business and patient PHI. Consider minimizing the use of noncredentialed or nonlicensed individuals in temporary positions if they are not bound by professional codes of conduct or ethics.
2. Minimize the use of Social Security numbers for identification: whenever possible, redact or replace some of the digits in the Social Security number; avoid displaying the entire number on any document, screen, or data collection field.
3. Store patient PHI in a secure manner, ensuring physical safeguards are in place such as restricted access and locks. Consider securing a release of liability from patients who refuse to use facility-provided lock boxes or other storage for their valuables, including wallets and purses.
4. Implement and comply with organizational policies for the appropriate disposal, destruction, and reuse of any media used to collect and store patient PHI.
5. Implement and comply with organizational policies and procedures that provide safeguards to ensure the security and privacy of patient PHI collected, maintained, and transmitted electronically. At a minimum:

    - Limit access to electronic PHI to a need-to-know basis and establish minimum necessary access controls
    - Require unique user identification and password controls
    - Implement encryption practices for transmitting patient PHI
    - Install appropriate hardware and software protective mechanisms such as firewalls and protected networks
    - Audit routinely to determine appropriate access to information, including access to PHI by staff with a newly assigned user ID

6. Train staff on organizational policies and practices developed to provide protection and appropriate use and disclosure of patient PHI, as well as appropriate responses to identity theft events.
7. Develop a proactive identity theft response plan or policy that clearly outlines the response process and identifies the organization's obligations to report or disclose to law enforcement or government agencies information related to such crimes:

    - Identify federal and state laws applicable to identity theft, reporting, and disclosing
    - Complete a preemption analysis addressing HIPAA's permitted disclosures to law enforcement (§164.512(2)(5)) versus state law, determining when there is a need for court order, subpoena, or patient authorization

Responding to an Identity Theft Event

Upon determining that an identity theft has occurred, the organization should respond prompty with the following steps.

Initiate an internal investigation immediately to review the facts. This should include a strategy for both investigation and communication. A team of individuals appropriate to the investigation should be assembled, with one individual assigned the role of team leader. The team may include:

- Administration
- Privacy officer
- Security officer
- Risk management
- Compliance officer (as needed)
- Legal counsel (as needed)
- Corporate resources (as needed)
- Media relations (as needed)
- Human resources (as needed)
- Facility security or plant operations (as needed)

Determine internal operational steps. The investigative team should determine if steps should be taken to:

- Identify and sequester pertinent medical records, files, and other documents
- Suspend billing processes until the matter has been resolved
- Process appropriate amendments or corrections once the matter has been resolved

Notify local law enforcement authorities. Once it has been determined that the identity theft event could result in harm to a person or business, the organization should notify local law enforcement authorities. Disclosure to law enforcement agencies is permitted under HIPAA §164.512(l)(5). A covered entity may disclose PHI to law enforcement officials if the covered entity believes in good faith there is evidence of criminal conduct that occurred on the premises of the covered entity. However, before disclosure of PHI to law enforcement agencies, state law should also be considered. Healthcare organizations should not disclose PHI unless authorized by the patient or in response to a legal court order unless state law dictates otherwise. Healthcare organizations may want to seek legal counsel for assistance with identity theft events. Based on the scope of the identity theft event, the organization may also want to notify:

- FTC
- Federal Bureau of Investigation
- Social Security Administration or the Inspector General

Notify individuals. The organization should consider immediate notification of those individuals whose personal information has been compromised. This will allow them to take steps to mitigate the misuse of their information. Prior to notification the organization should consult with the law enforcement contact about the timing of the notification so it does not impede the investigation. The following factors should be considered when deciding if notification is warranted:

- Nature of the compromise
- Type of information taken
- Likelihood of misuse
- Potential damage arising from misuse

A designated person within the organization should be charged with reporting or disclosing information and notifying victims of the identity theft. This person should be provided with the latest information about the theft, the organization's response, and the guidance available for the victims. All disclosures made as a result of identity theft should be accounted for and included in any future requests by the patient for an accounting of disclosures.

Should the organization consider communication to those victims whose information may have been compromised, the FTC has provided the following guidance for developing the notification:

- Describe clearly what is known about the compromise. Include how it happened; what information was taken and, if known, how the thieves have used the information; and what actions have been taken already to remedy the situation. Explain how to reach the contact person in the organization. Consult with the law enforcement contact on exactly what information to include so the notice does not hamper the investigation.
- Explain what responses may be appropriate for the type of information taken. For example, people whose Social Security numbers have been stolen should contact the credit bureaus to ask that fraud alerts be placed on their credit reports. Visit www.consumer.gov/idtheft for more complete information on appropriate follow-up after a compromise.
- Include current information about identity theft. The FTC's Web site, www.consumer.gov/idtheft, has information to help individuals guard against and deal with identity theft.
- Provide contact information for law enforcement officers working on the case (as well as the case report number, if applicable). Alert law enforcement officers working on the case that the contact information is being shared. Identity theft victims often can provide important information to law enforcement. Victims should request a copy of the police report and make copies for creditors who have accepted unauthorized charges. The police report is important evidence that can help absolve a victim of fraudulent debts.
- Encourage those who discover that their information has been misused to file a complaint with the FTC at www.consumer.gov/idtheft or by calling (877) ID-THEFT (438-4338). Information entered into the FTC's database, Identity Theft Data Clearinghouse, is made available to law enforcement.[1]

Determine a communications response. The organization should work with law enforcement, legal counsel, and corporate resources to determine the need for a media release or response to an identity theft event.

Debrief. Following resolution of the identity theft, the investigative team should meet to review the event, identify the risk factors, assess the organization's response, determine appropriate future safeguards and preventions, and assign responsibility for follow-up.

Credit Bureaus		
Equifax Fraud Reporting (800) 525-6285 P.O. Box 740241 Atlanta, GA 30374-0241	Experian Fraud Reporting (888) 397-3742 P.O. Box 9532 Allen, TX 75013	TransUnion Fraud Reporting (800) 680-7289 Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790

Assisting the Victim of an Identity Theft

The FTC provides very specific guidance to victims of identity theft on its Web site, www.consumer.gov/idtheft, where brochures (available in English and Spanish) titled "ID Theft: What's It All About" can be downloaded in text form or as PDF files. Identity theft victims should follow up all calls in writing and send correspondence by certified mail (return receipt requested) so there is documentation as to what the company received and the date. Copies should be retained in the victim's personal files.

Organizations can assist victims of identity theft by encouraging victims to:

1. Immediately place a fraud alert on credit reports. Victims may call the fraud number of any of the three major credit bureaus toll-free to place a fraud alert on their credit report (see box). This alert can help prevent an identity thief from opening additional accounts in the victim's name. As soon as the credit bureau confirms the fraud alert, it will automatically notify the other credit bureaus. The credit bureaus will forward credit reports to victims free of charge.
2. Once the credit reports are received, the victim should review them carefully. Discrepancies and errors should be reported to the credit bureau as soon as possible.
3. The victim should immediately close any accounts that have been tampered with or opened fraudulently, which may include bank accounts, credit cards, loans, phone company accounts, utility accounts, Internet service provider accounts, or other service providers. The FTC, in conjunction with banks, credit grantors, and consumer advocates, developed an ID theft affidavit to help victims close unauthorized accounts and get rid of debts wrongfully attributed to them. If victims don't have a police report or any paperwork from creditors, they should send the completed affidavit to the three major credit bureaus. The bureaus will use it to start the dispute investigation process. Not all companies accept the affidavit; some may require the victim to use their forms instead.
4. The victim should file a report with the law enforcement agencies in the community where the identity theft took place. The victim should maintain a copy of the report to validate claims with creditors. Victims should follow these tips for filing a police report:

    - Furnish as much documentation as possible to prove the case. Debt collection letters, credit reports, a notarized ID theft affidavit, and other evidence of fraudulent activity can help demonstrate the case's seriousness.
    - Be persistent if local authorities say they can't take a report. Stress the importance of a police report; many creditors require one to resolve disputes. Remind them that credit bureaus will automatically block the fraudulent accounts and bad debts from appearing on credit reports, but only if they receive a copy of the police report.
    - If told that identity theft is not a crime under state law, ask to file a miscellaneous incident report instead.
    - If the local police won't take a report, try the county police. If that doesn't work, try the state police.
    - Some states require the police take reports for identity theft. Check with the state attorney general to find out what states have this law.[2]

5. The victim should file a complaint with the FTC to provide information that can assist law enforcement officials in tracking down the identity thieves. The FTC may also refer victims' complaints to other government agencies and companies for further action. Victims may file a complaint with the FTC by letter, phone, or Web:

    Identity Theft Clearinghouse
    Federal Trade Commission
    600 Pennsylvania Avenue, NW
    Washington, DC 20580
    www.consumer.gov/idtheft

(877) IDTHEFT (438-4338)
TDD: (202) 326-2502

Resolving Identity Theft and Ensuring the Accuracy of Personal PHI

Individuals who believe they have been the victims of identity theft and wish to ensure the accuracy of their health records and PHI should request to view or receive a copy of their health records

They should report any information they believe is inaccurate to the organization's privacy officer or HIM department. They should also make a request for amendment to the paper and electronic medical records. The request should include addresses of healthcare providers and insurance carriers that should be contacted with corrected information, when and if the request is approved. The victim should provide copies of supporting documentation with the amendment (e.g., police reports, the affidavit of identity theft, letters to and from creditors).

If the request for amendment is denied, the victim should appeal the request and ask that any further requests for information include the initial request and appeal information. Healthcare providers should be contacted in writing to ensure that care and treatment are not based on false information. Individuals should keep copies of all correspondence or forms sent in their personal files.

Identity theft crimes will continue to affect healthcare organizations. HIM professionals should be leaders in their organization in the development of preventive practices to reduce the risk of identity theft and fraud. It is important to respond appropriately to identity theft and be knowledgeable about when and how to notify the victims, local law enforcement, and appropriate federal agencies. HIM professionals must have a clear understanding of HIPAA and federal and state laws, knowing when and how to disclose patient PHI. And HIM professionals should cooperate to the fullest extent in the investigation of identity theft or fraud incidents.

Notes

1. Federal Trade Commission. "Information Compromise and the Risk of Identity Theft: Guidance for Your Business." Available online at www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.htm.
2. FTC. "Take Charge: Fighting Back against Identity Theft." Available online at www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.

References

Allina Hospitals and Clinics, and Health Care Compliance Association. "Identity Theft: The Next Generation of Concerns for a Compliance Officer." Presentation at the HCCA Annual Conference, Chicago, IL, April 2004.

Federal Trade Commission. "ID Theft Home." Available online at www.consumer.gov/idtheft.

Cavanaugh Baes, Michael, and Vickie McCormack. "Identity Theft: What It Is, How to Prevent It, and What to Do if It Happens." *Compliance Today*, January 2004.

"Healthcare Compliance Officers Tackle Identity Theft Issues." *Report on Medicare Compliance* 12, no. 41 (2003).

"Identity Theft and Assumption Deterrence Act of 1998." Public Law 105-318. October 30, 1998. Available online at www.ftc.gov/os/statutes/itada/itadact.htm.

Prepared by

Nancy Davis, MS, RHIA
Chrisann Lemery, MS, RHIA
Kim Roberts, MSA, RHIA, CHP

Acknowledgments

Jill Burrington-Brown, MS, RHIA
Michelle Dougherty, RHIA, CHP
Rose Dunn, CPA, RHIA, FACHE
Beth Hjort, RHIA, CHPS
Carol Ann Quinsey, RHIA, CHPS

Article citation:
Davis, Nancy, Chrisann Lemery, and Kim Roberts. "Identity Theft and Fraud-The Impact on HIM Operations (AHIMA Practice Brief)." *Journal of AHIMA* 76, no.4 (April 2005): 64A-D.