MEDICAL IDENTITY THEFT

FAQs for Health Care Providers and Health Plans

FEDERAL TRADE COMMISSION | business.ftc.gov

Although identity theft is usually associated with financial transactions, it also happens in the context of medical care. According to the Federal Trade Commission (FTC), medical identity theft occurs when someone uses another person's name or insurance information to get medical treatment, prescription drugs or surgery. It also happens when dishonest people working in a medical setting use another person's information to submit false bills to insurance companies.

Medical identity theft is a concern for patients, health care providers, and health plans. Health care providers and insurers are asking how they can minimize the risk and help their patients if they're victimized. Here are the FTC's answers to those questions.

HOW WOULD PEOPLE KNOW IF THEY'RE VICTIMS OF MEDICAL IDENTITY THEFT?

Victims may:

- get a bill for medical services they didn't receive;
- be contacted by a debt collector about medical debt they don't owe;
- see medical collection notices on their credit report that they don't recognize;
- find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- be told by their health plan that they've reached their limit on benefits; or
- be denied insurance because their medical records show a condition they don't have.

WHAT SHOULD I DO IF I LEARN THAT A PATIENT MAY BE A VICTIM OF MEDICAL IDENTITY THEFT?

Conduct an investigation. For example, if your billing department gets a call from a patient who claims she was billed for services she didn't receive, review your records relating to the services performed and any supporting documentation that verifies the identity of the person receiving the services. You also should review the patient's medical record for inconsistencies.

If you determine there was medical identity theft, notify everyone who accessed the patient's medical or billing records. Tell them what information is inaccurate in the patient's files, and ask them to correct the records.

Understand your obligations under the Fair Credit Reporting Act (FCRA). If you report debts to credit reporting companies, determine how the identity theft affects your responsibilities under the FCRA. For example, if the patient gives you an identity theft report detailing the theft, the FCRA says you can't report any debt associated with the theft to the credit reporting companies. An identity theft report is a police report that contains enough detail for the credit reporting companies and the businesses involved to verify that the consumer is a victim. The report also states which accounts and inaccurate information resulted from the theft.

For more information about your obligations under the FCRA, visit **ftc.gov/idtheft**.

Review your data security practices. Even if the information used to commit the fraud didn't come from your organization, it's a good reminder that you need to periodically review your data security practices and your compliance with the information safeguard provisions of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.

For more information, see *Protecting Personal Information: A Guide for Business* (**ftc.gov/infosecurity**) and guidance from the Department of Health and Human Services on HIPAA compliance, at **hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html.**

Provide any necessary breach notifications. If your investigation reveals that your organization improperly used or shared protected health information (for example, if an employee improperly used health information to commit medical identity theft or if health information was improperly shared with an identity thief), you should determine whether a breach occurred under the HIPAA Breach Notification Rule (45 CFR part 164 subpart D) or any applicable state breach notification law.

WHAT SHOULD I TELL A PATIENT WHO'S A VICTIM OF MEDICAL IDENTITY THEFT?

Here are some practical tips to help your patient correct medical, billing, and financial records.

If you are covered by HIPAA, make sure the patient has a copy of your Notice of Privacy Practices. The Notice should include contact information for someone in your organization who can respond to questions or concerns from patients about the privacy of their health information. You also may put the person in touch with a patient representative or ombudsman.

Advise the victim to take advantage of his rights under the HIPAA Privacy Rule.

✓ **The HIPAA Privacy Rule gives people the right to copies of their records maintained by covered health plans and medical providers.** Patients may ask for copies of their medical and billing records to help identify the impact of the theft, and to review their records for inaccuracies before seeking additional medical care. There is no central source for medical records, so patients need to contact each provider they do business with – including doctors, clinics, hospitals, pharmacies, laboratories and health plans. For example, if a thief got a prescription filled in your patient's name, the victim may want the record from the pharmacy that filled the prescription and the health care provider who wrote the prescription. Explain that there may be fees and mailing costs to get copies of medical or billing files.

Some medical providers and health plans believe they would be violating the *identity thief's* HIPAA privacy rights if they gave victims copies of their own records. That's not true. Even in this situation, patients have the right to get a copy of their records.

✓ **Patients have the right to have their medical and billing records amended or corrected.** Encourage patients to write to their health plan or provider to dispute the inaccurate information. Tell them to include copies (they should keep the originals) of any documents that support their position. Their letter should identify each disputed item, the reasons for disputing it, and a request that each error be corrected or deleted. Patients may want to include a copy of their medical or billing record with the items in question circled.

The originator of the information must correct the inaccurate or incomplete information, and notify other parties, like labs or other health care providers, that it knows received the incorrect information. If an investigation doesn't resolve the dispute, patients can ask that an explanation of the dispute be included in their records.

✓ **Patients have the right to an accounting of disclosures from their medical providers and health plans.** An accounting of disclosures may help indicate to patients whether there has been an inappropriate release of their medical information. An accounting is a report of certain disclosures made of the patient's medical information by the medical provider or health plan. Although some disclosures that occur often or as a matter of routine – for example, a doctor's disclosure of treatment information to another health care provider or payment information to an

insurer for reimbursement – do not need to be included in the accounting, it would include information that may be helpful, like misdirected faxes or e-mails or any information released based on an invalid patient authorization.

The law allows your patients to order one free copy of the accounting from each of their providers and health plans every 12 months. The accounting is a record of:

- the date of the disclosure;
- the name of the person or entity who received the information;
- a brief description of the information disclosed; and
- a brief statement of the purpose of the disclosure or a copy of the request for it.

✓ **Patients have the right to file a complaint if they believe their privacy rights have been violated.** For example, it would be a violation if a medical provider refused to provide someone with a copy of his or her own medical record. Patients can file a complaint with the U.S. Department of Health and Human Services' Office for Civil Rights, at **www.hhs.gov/ocr.**

Encourage your patients to notify their health plan if they suspect medical identity theft. Getting a list of benefits paid in their name can help your patients determine whether there are any fraudulent charges. Patients also should read their Explanation of Benefits (EOB) statements that health plans send after treatment, and check that the claims paid match the care they received. They also should verify that the name of the provider, the dates of service, and the services provided are correct. Patients should report discrepancies to their health plan.

Tell your patients to file a complaint with the FTC at **ftccomplaintassistant.gov** or by phone at 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261, and to check out the information at **ftc.gov/idtheft.** They also should file a report with local police, and send copies of the report to their health plan's fraud department, their health care provider(s), and the three nationwide credit reporting companies. Information on how to file a police report and reach the credit reporting companies is at **ftc.gov/idtheft.**

Encourage your patients to look for signs of other misuses of their personal information. Someone who engages in medical identity theft also may use their victim's personal information to commit more traditional forms of identity theft, like opening a credit card account in the victim's name. Tell your patients to order copies of their credit reports, and to review them carefully. Credit reports are full of information, including what accounts people have and whether their bill paying is timely. The law requires each of three major nationwide credit reporting companies – Equifax, Experian and TransUnion – to give people a free copy of their credit report each year if they ask for it at **www.AnnualCreditReport.com** or from1-877-322-8228.

Once victims have their reports, they should look for inquiries from companies they didn't contact, accounts they didn't open, and debts on their accounts that they can't explain. They also should check that their Social Security number, address(es), name or initials, and employers' names are listed correctly. If they find inaccurate or fraudulent information, they can visit **ftc.gov/idtheft** to learn how to get it corrected or removed.

HOW CAN I HELP MY PATIENTS DETER, DETECT, AND DEFEND AGAINST MEDICAL IDENTITY THEFT?

You can provide the FTC's brochure, *Medical Identity Theft* (**consumer.ftc.gov/articles/0171-medical-identity-theft**). It explains how medical identity theft occurs and how it differs from traditional identity theft, and it offers tips on how to minimize risk and how to recover if a theft occurs. The brochure is available in English and Spanish. The FTC encourages you to print copies and to make them available to your patients. You also may link to the brochure, copy it, or adapt it for your website or newsletter.

Additionally, the HIPAA Privacy and Security Rules include a number of requirements that, when followed, will substantially reduce the risk of medical identity theft. For example, the Privacy Rule requires HIPAA covered entities to verify the identity of persons requesting protected health information and to have reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information, like training employees on how to handle and dispose of health information, and how to keep health information physically secured.

About the FTC

The FTC works to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or get free information on consumer issues, visit **ftc.gov** or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a new video, *How to File a Complaint,* at **ftc.gov/video** to learn more. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to **www.sba.gov/ombudsman.**

Federal Trade Commission
BCP Business Center
business.ftc.gov
January 2011