Tips for Consumers to Reduce Medical Identity Theft and Fraud

What are Medical Identity Theft and Medical Identity Fraud?
Both terms refer to crimes that involve the theft of Personally Identifiable Information (PII) from another individual. In the case of medical identity theft, this also includes Protected Health Information (PHI) – such as name, date of birth, social security number, health plan number and medical records. Fraud indicates the stolen PHI was used for personal gain by another individual, such as from the sale of PHI to others or from the use of PHI to obtain medical goods and services. Perpetrators commit this crime to obtain unauthorized insurance benefits, prescription drugs, medical services, employment, government benefits or other financial gain.

The incidence and consequences of medical identity theft continue to rise. A recent study by the Medical Identity Fraud Alliance (MIFA) indicates this type of fraud has nearly doubled since 2010. There were more than 2.3 million adult victims of medial identify fraud in the U.S. in 2014. Out-of-pocket costs to victims have grown, with twice as many victims experiencing out-of-pocket costs to correct their medical identities and deal with the resulting problems, at an average of $13,500 per victim.

A serious threat to victims is contamination of their health records with erroneous information from the identity thief, including, blood type, serious health conditions and prescription or illegal drug use. Victims can experience serious risks related to their healthcare such as misdiagnosis, mistreatment and delayed care due to incorrect medical records.

Help protect yourself against this costly and potentially life-threatening type of identity fraud:

- Carefully review Explanations of Benefits from your health plan. Immediately report any incorrect items, such as a hospital visit you never made or prescriptions that are not yours.
- Monitor billing statements from healthcare providers. Unfamiliar charges for medical procedures, products or pharmaceuticals may suggest someone has committed fraud.
- Periodically check with your physician(s) to ensure the accuracy of your medical records. Make sure they accurately reflect your medical history and treatment. Look for inaccurate details such as incorrect blood type, pre-existing conditions, allergies, etc., which may belong to the identity thief.
- Don't be afraid to ask your healthcare provider about protecting your PHI:
  - How are your digital systems that contain my PHI secured? How do you prevent external and internal intrusions into your records and databases?
- Do not share your medical identity, such as your health insurance plan, with other individuals. Sharing your health plan ID for another to use is healthcare fraud.
- Protect your medical identity as you would any other sensitive information, such as your financial credentials. This includes disposing/shredding of health documents you no longer need.
- Do not provide your medical information over the phone or via email unless you verify the entity on the other end.
- If you wear personal health devices, use healthcare-related websites or mobile apps, be sure you know how that company is storing and protecting your personal data. Most of these companies are not regulated in the same way as your healthcare provider or health plan to protect your PHI.
- Be careful not to overshare your health-related matters on social media – fraudsters are extremely good at aggregating information about you to create a "complete" medical identity profile, which can then be exploited for their financial gain, at cost to you.

This information presented by the Medical Identity Fraud Alliance (MIFA). To learn about MIFA, contact Ann Patterson at 703-407-0958 or Ann@MedIDFraud.org, or visit us at www.MedIDFraud.org.