## SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

# Hackers: Bad for Your Health Care

**YOUR CREDIT CARD** information is still tempting bad-guy bait, but it turns out your health care data can be even more valuable. Financial data has a finite lifespan—it becomes worthless the second the customer detects the fraud and cancels the card or account. Information contained in health care records has a much longer shelf life and is rich enough for identity theft. Social Security numbers can't easily be canceled, and medical and prescription records are permanent. There's also a large market for health insurance fraud and abuse.

Health care breaches aren't typically discovered through black market sales of personal data, the way retail breaches often are, because criminals monetize health care data in a different way than they cash in on financial data. Stolen health care data forums operate kind of like drug cartels, where health records are not sold outright, but rather used to buy and sell addictive prescriptions, said Angel Grant, senior manager for antifraud solutions at security provider RSA. "Health insurance credentials are especially valuable in today's economy because health care costs are causing people to seek free medical care with these credentials," Grant said.

**Here's how to keep your health care data safe**:

■ **Review your medical treatment records** regularly to make sure that only services you actually received are documented.

■ **Be cautious any time you are asked to provide** your name, address, date of birth or Social Security number. Very few entities are truly entitled to that information.

■ **Read the explanation of benefits statement** that your health plan sends after treatment. Check the name of the provider, the date of service, and the service provided to ensure that the claims paid match the care you received. If you see a mistake, contact your health plan.

■ **Review your credit report and credit card statements** regularly to check for bills or collection accounts for unknown medical services.

■ **Don't share medical or insurance information** by phone or email unless you initiated the contact and know whom you're dealing with. Medical identity thieves may pretend to represent an insurance company, doctors' office or pharmacy to try to trick you into revealing sensitive information.

■ **Keep paper and electronic copies** of your medical and health insurance records in a safe place. Shred outdated health insurance forms, prescriptions, physician statements, and prescription bottle labels before discarding them.

**If you suspect your health care data has been compromised:**

■ **File** a police report immediately.

■ **Notify** all your medical service providers and insurance providers. Have them note the incident on your records and correct any erroneous information.

■ **Place** a security freeze or fraud alert on your credit files with all three major credit bureaus (Equifax, Experian and TransUnion).