

Karen Telleen-Lawton: Sustainable Privacy

Ward off medical identity theft by safeguarding what you disclose and to whom

By [Karen Telleen-Lawton, Noozhawk Columnist](#) | Published on 05.31.2010

My 39-year-old sister-in-law died of identity theft in 1995. Her death certificate listed “breast cancer” as the cause, but I believe her illness was exacerbated by this stress. Thieves used her name to charge everything imaginable in the last few years of her life. When I’d visit or take her to doctor’s appointments, she was often trying to deal with the mess.

Passage of the health-care bill heralds increasing requirements for medical companies to improve efficiency and accuracy by computerizing medical records. In the wake of this computerization, computer thieves are busy operating at several different levels, according to the [AARP](#):

» Medical identity theft has more than doubled since 2008, to more than a million victims in the past two years. Security analyst [Robert Vamosi](#) says, “Medical records are the mother lode for identity thieves, who call them ‘fulls’ because they contain everything that’s needed to establish someone else’s ID — [Social Security](#) numbers, addresses, sometimes payment accounts.”

» “Friendly fraud” is the euphemistic term for insureds who lend their insurance cards to uninsured loved ones. They typically end up with an average out-of-pocket cost of \$20,000 to resolve their medical fraud cases.

» A “mole” in physician or insurance offices may steal patient records for gain.

Businesses with sensitive information strain to stay ahead of internal and external break-ins. Some, such as banks, are required to have security checks twice per year. An industry has developed to point out cracks in client privacy protection for communications giants, satellite and technology companies, and medical and insurance companies.

One such company is Carpinteria-based [Redspin](#), which has helped clients protect their customers’ information since 2000. Redspin’s “professional hackers” offer “information penetration testing and security assessment services that provide an effective technical solution tailored to your business context.” (Disclosure: My husband has worked there since 2006.)

Security assessment professionals work on the business side, but it’s up to us to protect what we disclose. Perhaps that’s why I’m a stickler about not offering up my Social Security number when I’m asked to provide it. The [Privacy Act](#) regulates the use of SSNs. A government agency requesting it must inform you whether disclosure is mandatory, how they will use it and disclose the consequences for refusing.

You can refuse to supply your SSN to any business, though you risk doing so without the product or service you’re trying to obtain. The company may seek the number to do a credit check, but they don’t really need your SSN.

The AARP provides a list of steps to cut down on medical identity theft. These include:

- » Urge your health-care providers to ask patients for photo identification.
- » Ask your doctors to make copies of everything in your medical file (you may have to pay this cost).
- » Read every letter you get from insurers, including “this is not a bill” statements. If a doctor’s name or treatment date isn’t familiar, call the billing physician and your insurer.
- » Ask for a list of benefits paid in your name and an “accounting of disclosures,” which shows who received your records.
- » Monitor your credit report at AnnualCreditReport.com. If you see medical billing errors, contact your insurer and the three credit bureaus: [Equifax](http://Equifax.com), [Experian](http://Experian.com) and [TransUnion](http://TransUnion.com).
- » Obscure the last four digits of your SSN from insurance cards in your wallet. If you lose your insurance card, contact your insurance provider.

To these I would add a couple more caveats. One tip, urged by the [Social Security Administration](http://SocialSecurityAdministration.gov), is always to question why your SSN is being requested, deciding based on the answer whether to disclose it. Second, avoid sending more information into cyberspace than you would be comfortable sharing with any employer, service provider or other person on the planet.

Information divulgers, beware! The life thrown into chaos may be your own.

— *Karen Telleen-Lawton's column is a mélange of observations supporting sustainability. Graze her writing and excerpts from Canyon Voices: The Nature of Rattlesnake Canyon at www.CanyonVoices.com.*