MASSACHUSETTS MEDICAL SOCIETY

Securing Your Identity:
Prospective and Retrospective Considerations

October 23, 2009

Prepared by
Adam Shlager
Manager, Health Systems
Massachusetts Medical Society
Physician Practice Resource Center
860 Winter Street
Waltham MA 02451
800-322-2303 x7702
ashlager@mms.org

This information is intended to serve as a general resource and does not constitute legal advice. If you need legal advice, please consult an attorney.

Identity Security – Prospective and Retrospective Considerations

Anyone who has had their identity stolen knows the sense of loss and panic that accompanies. It is imperative that action take precedence.

There are some actions you might want to consider to try to maintain the security of your information.

Risk Areas:

The Internet and your computer: If you use the internet and have any accounts available anywhere, you have data at risk. The Internet and electronic data are highlighted as primary areas of risk in this resource, but socially engineered data loss is also widespread and should not be discounted.

Professional listings:

   a. Memberships often have significant information available, self-listed and aggregated by automated programs that troll the internet for this information.
   b. May be listed secondarily with associated information (e.g, CMS NPI site lists physician NPI, license number, type of corporation worked for, address, phone number, Medicare PIN, Medicaid number, etc)
   c. Provider listings by plans and hospitals may have significant information available

2. Social networking sites – often contain significant personal information in profiles.
   a. Linked In
   b. Facebook
   c. Twitter
3. Any and all accounts used for purchases and/or bill payment.
   a. While secure, these are standard targets for identity theft
4. Your own computer
   a. This applies to both PC and Mac users. While PC viruses, Trojans and other malware are well known, Macs are coming under increased scrutiny as evidenced by a web-site recently taken down that offered a 43 cent per Mac incentive for infected machines.
5. Your Smartphone
   a. All Smartphones have vulnerabilities that are well documented and published. This covers Windows Mobile, Android and the iPhone. A recent article exposed the algorithm for breaking encryption on all phones.

The more data elements any ill-intentioned entity has, the more likely they will be able to use that data to their advantage.

As portable devices continue to converge towards non-location specific (cloud) micro-computing, there will continue to be security challenges.

While there is currently no way to control external entities beyond existing legislative and regulatory guidance, there are certainly steps that might be taken to control the extent of any loss of data, and mitigate the effect of identity theft after the fact. Nothing will protect data absolutely, but there are steps that may be taken to ameliorate the plethora of data warehousing tactics that exist online.

As a side note, well before the advent of internet consumption, a data breach occurred in Virginia approximately 10 years ago that was traced back to a group of indigent persons who trolled neighborhood mailboxes and simply picked out credit card and other financial offers. This led to significant losses without the benefit of the internet data. For years, diners have handed over their credit cards to wait staff, who then walk out of view where they record the credit card information electronically on a terminal. These examples are intended to show that protecting your identity is not necessarily associated exclusively with the data explosion and web use.

Identifying and Reducing Risks

As the last examples demonstrate, there is no effective way to eliminate the risk of identity theft. As long as there is someone willing to exploit information with knowledge, incentive, and inclination, there will be risks associated. Now that you know where your data might be, here is a partial list of opportunities that might assist you in reducing your exposure, and help you make decisions about your preferences in sharing and securing information.

1. Eliminate or secure the administrator account on laptops.
2. Require a secure log on to any portable device. This includes thumb drives, SD cards, etc.
3. Keep all operating systems up to date with patches, security updates, etc.
4. Use anti-virus/malware products and keep up to date.
5. Use different passwords and IDs to log in across different sites.
6. All purchases on line may be made discreetly and information not stored for the next purchase, i.e. do not set up accounts on line to minimize data stored.
7. Log in to any financial accounts maintained online (savings, checking, credit, loans, etc) at least weekly to monitor for unusual activity.
8. Lock down all social/business networking information available to the general public.
9. Inspect friend/networking invitations before accepting and make sure they are bona fide.
10. Do not respond to general delivery e-mails asking you to log into any account, or click links within the e-mail. Open a separate browser window and go to the site directly if you believe you need to confirm information.
11. Secure sensitive documents by encrypting them. If they are to be e-mailed and secure e-mail is not available, encrypt the document.
12. Google yourself. This simple exercise will show you what information is quickly available, and the depth of that information. In some cases, you may be able to request withdrawal of some information by the web site administrator, and there are some entities that specialize in reducing web presence.
13. Avoid using your SSN as an identifier whenever possible. This includes on your driver's license, as your business Tax ID, or anywhere else it's avoidable.

For physicians especially, there are significant risks because of the sheer volume if information available about them through affiliations. Hospitals and health plans list physicians and some details about them. Also, previously mentioned, CMS lists quite a bit of information about physicians in their NPI enumeration look-up system. Know where your information is held, and make sure you are comfortable with the security in place that is protecting it.

Sometimes one or two elements of information can lead to the extrapolation of related information. For instance, algorithms have been developed which extrapolate social security numbers from an

individual's birthplace, which comprises the first three digits and is widely available for a variety of sources. Some of these sources may be under your control, such as the social networking sites.

The same procedure applies in all cases. Any time you publish information about yourself online in any method or modality (profile, tweet, etc), you should think about what the information might be used for and who might have access to it. If you have hardware, you should secure it by all means available and make sure it remains physically secure at all times.

If Data Has Been Stolen or is Suspected to Have Been Stolen

If you are notified that your information or data has been or may have been compromised, there are some steps that should be taken immediately. It may be a natural reaction to call the entity responsible and demand answers, but that should be secondary to taking steps to protect yourself and your information. None of these suggestions obviate the need for any of the suggestions in the mitigating risk section above.

1. Call one of the three credit centers (Experian, Equifax, Trans Union) and request an immediate fraud alert be placed on your credit. This alert should be in place for a minimum of one year.
2. Find out exactly what information may have been compromised and scan records to determine where that information might be available from other sources. Bank information may be linked to specific accounts.
3. Replace credit/debit cards as necessary.
4. If you are using your SSN as your corporate identifier, file for a Tax ID number.
5. Request and review any additional information from the breached source, such as response to the breach, additional steps or recommendations they might have, and what they are doing to prevent this in the future.

Conclusions

Identity protection will need to become second nature to individuals that participate in the electronic evolution of this century. The first step is realizing how pervasive our own information has become through electronic listings from high school reunions to our professional lives, and understanding how electronic information may be cached and stored indefinitely.

Reducing threat opportunities when possible and reducing response times to suspected breaches will help individuals mitigate risks. Consistent and regular monitoring of all accounts and information held online or in electronic form will also contribute to reducing risks. Ultimately, it is important to acknowledge that the risks may originate from multiple points and may largely be out of the individual's locus of control. Some of the ideas mentioned in this resource may help expand the locus of control by restricting the unnecessary availability of data.