Identity Theft

A Core Risk of HIPAA Security Lapses

Gail Sausser

Table of Contents

Show Me The Money

- **Willie Sutton, a notorious American bank robber of a half century ago, was once asked why he persisted in robbing banks. *"Because that's where the money is."***

Willie Sutton
FBI Photo

- **The money is now in identity theft!**

Identity Theft and Health Care Providers

- **Identity theft is now the number one financial crime in the country, and health care organizations are prime targets because of the large amount of personal data that is open to thousands of employees, contractors, and off site providers.**

Identity Theft and Health Care Providers

- **“Health care organizations are vulnerable because they have both a lot of low-paid workers and a lot of sensitive patient information.”**

  HIPAA Compliance Strategies, Report on Patient Privacy, June 2005, http://www.aishealth.com/Compliance/Hipaa

- **“Because physician offices tend to be harbors of sensitive information, not only about the doctors but about thousands of patients, they are often targeted.”**

- AMANews, Safeguarding identity: Tips to stave off a growing problem, June 26, 2006, http://www.ama-assn.org/amednews/site/free/bisa0626.htm

Hospital Identity Theft

- **A nurse in a Philadelphia hospital gave terminally ill patients' identities to a crime ring. They drained the patients' accounts and obtained $10 million in fraudulent mortgages using the stolen personal information.**
- Source, Bob Sullivan, Hospital ID theft: How to protect yourself, 12/23/05 http://redtape.msnbc.com/2005/12/hospital_id_the.html

Hospital Identity Theft

- **An employee at a Seattle cancer care center stole patient identities, obtained fraudulent credit in their names and ran up debt.**
- ***"Dateline NBC will tell the incredible story of a man sick with a terrible form of leukemia, a man literally days from his death -- and the repulsive crime he suffered while enduring everything else that comes with cancer. … While … was gasping for life, his imposter was living it up on fraudulent credit cards."***
- Source, Bob Sullivan, Hospital ID theft: How to protect yourself, 12/23/05 http://redtape.msnbc.com/2005/12/hospital_id_the.html

Yale New Haven Hospital

- **Hospital emergency room records were the source of identity theft.**
  - ***"You're panicking worrying about him and they are asking your name address, social security number insurance form, and you are at a vulnerability point and you just give it away and never realize someone is going to use that information against you,"* quoting a man whose son was a victim.**
- **Police arrested an employee of Yale Medical School who had access to hospital records. She allegedly gave patient information to her husband who pleaded guilty to identity theft charges last February.**

Source Alan Cohn, Team 8, Police connect hospital to identity theft cases 5/25/05, http://www.wtnh.com/Global/story.asp?S=3394079

Employee Theft

- In 2002, an employee at one of Allina's hospitals stole 32 patient Social Security numbers and gave them to her boyfriend, a gang member, who sold them for $100 each.
- To get the Social Security numbers, the employee confiscated inpatients' "blue cards," used to label medical records which contain patient names, addresses, birth dates and Social Security numbers. The private data was used to obtain credit cards in the patients' names.
- The employee pleaded guilty in the case and testified against other perpetrators. The hospital stopped using blue cards.
- Reported in HIPAA Compliance Strategies, Report on Patient Privacy, June 2005.

Employee Theft

- **An employee at Madrona Medical Group downloaded patient records, proprietary software, licensing keys and other data.**
- **Even after resigning, he continued to use his laptop to connect to its servers. He deleted backup files, e-mail files of the HR director, and server logs to cover his tracks.**
- **The Medical Group set up a patient help line and sent notice to thousands of patients recommending they:**
  - **File a fraud report with one of the credit bureaus**
  - **Request copies of their credit reports**
  - **Call businesses where their account have been tampered or opened fraudulently**

Mary Lane Gallagher, The Bellingham Herald, Aug. 11, 2006

Laptop Theft

- **The Providence Health Care hospital system revealed in Feb. 2006 that a laptop containing data on thousands of its patients had been stolen in Dec. 2005.**
- **The laptop was stolen from the van of an information services analyst. The thief broke open the van window to steal the data, which contained names, addresses, Social Security numbers, and medical diagnoses for patients in Providence's Home Care division.**

Laptop Theft

- **A computer belonging to Christus St. Joseph Hospital in Houston was stolen from the office of one of its vendors.**
- **The vendor had possession of the computer to convert paper records to electronic files. It contained patients' medical records and Social Security numbers.**
- **In April, the hospital sent 16,000 letters to patients saying that their Social Security numbers and medical records may be on a computer stolen from a hospital vendor, the newspaper reported.**
- **Reported in HIPAA Compliance Strategies, Report on Patient Privacy, June 2005.**

Laptop Theft

- **Kaiser Permanente mailed letters to 160,000 of its Northern California-based HMO subscribers, informing them that a laptop containing their personal information had been stolen.**
- **The data was being used to market Hearing Aid Services to Plan members.**
- **No social security numbers were on the laptop, which was stolen from a "secure office" in the Permanente Medical Group Business Development Group.**
- Ryan Singel and Kevin Poulsen, Kaiser Joins Lost Laptop Crowd, July 27, 2006, Wired News, http://attrition.org/dataloss/2006/07/kaiser01.html

Laptop Theft

- **The home care unit of William Beaumont Hospital offered a year of free credit protection service following the theft of a laptop computer with protected patient information.**

  The laptop was in a vehicle stolen on Aug. 5 in Detroit. The laptop, with information on more than 28,000 home care patients, was recovered Aug. 23 and a forensic expert determined no information was accessed. The hospital, however, will continue to offer the credit service.

  Patient data on the laptop included names, addresses, birth dates, medical insurance information, and Social Security numbers.

  The laptop was password-protected and encrypted, but the nurse using the laptop was recently hired and her ID access code and password were still with the computer.

- Health Data Management, Latest News, “Stolen Laptop Affects 28,000,” August 25, 2006

Laptop Theft

- About 8,000 clients of MD Management, a subsidiary of the Canadian Medical Association, received a letter from the company dated June 29 warning them that a laptop computer containing detailed information about their financial and professional circumstances had been stolen.
- "The car was in a shopping centre parking lot," he said. "The window was smashed. The contents of the car were stolen, including the laptop."

- Doctors angry after laptop stolen, July 26, 2006, Canadian Press, http://www.theglobeandmail.com/servlet/story/RTGAM.20060726.gtlaptop0726/BNStory/Technology/http://attrition.org/dataloss/2006/07/mdmgt01.html

Thumb Drives

- **The Social Security numbers of 130,000 former and current Wilcox Memorial Hospital patients were lost due to the disappearance of a thumb drive.**
- **The data of hospital patients includes names, addresses, medical record numbers and Social Security numbers going back 12 years.**
- **Hospital officials are concerned about potential identity theft, should the computer drive, which is much smaller than a cellular telephone, fall into the wrong hands.**
- **"We have discontinued the use of thumb drives for this type of information storage."**
- **Source *Andy Gross - The Garden Island, Thursday, Oct 20, 2005.***

E-Prescribing

- **Georgetown University Hospital suspended a trial program with an electronic prescription-writing firm last week after a computer consultant stumbled upon an online cache of data belonging to thousands of patients.**
- **The hospital had securely transmitted the patient data to e-prescription provider InstantDx. But an Indiana-based consultant accidentally discovered the data on InstantDx's computers while working to install medical software for a client.**
- **The leaked information included patients' names, addresses, Social Security numbers and dates of birth, but not medical data or the drugs the patients were prescribed.**
- Kevin Poulsen, E-Health Gaffe Exposes Hospital, July 25, 2006, http://www.wired.com/news/technology/0,71453-0.html

What is medical identity theft ?

- **Medical identity theft occurs when someone uses a person's name and identity -- including insurance information -- without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods.**
- **Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records.**
- **http://www.worldprivacyforum.org/medicalidentitytheft.html**

Medical Identity Theft

- **A Boston area psychiatrist made false entries in charts of individuals who were not his patients. He gave individuals diagnoses of drug addiction and abuse, severe depression and numerous psychiatric sessions which they did not actually have, then used their personal information to submit false bills to insurance.**
- **The victims, after learning of the crime, had difficulties getting the false information removed from their medical files.**
- **United States v. Skodnek, 933 F. Supp. 1108,; 1996 U.S. Dist. LEXIS 9788 (D. D. Mass. 1996). *Reported on World Privacy Forum***

Medical Identity Theft

- **One medical identity theft victim from Florida went for medical treatment and says she found that her medical files had been altered. She said that she discovered that an imposter had caused false entries on her file, including changes to her blood type.**
- **Comment of L. Weaver in Federal Trade Commission, Identity Theft Victim Assistance Workshop,(Aug.18, 2000) http://www.ftc.gov/bcp/workshops/idtheft/comments/weaverlind.htm reported on World Privacy Forum**

Medical Identity Theft

- **An Ohio woman, while working at a dental office, accessed protected patient information and used the information to phone in prescriptions to area pharmacies.**
- **According to the Office of Inspector General, Health and Human Service, she "called in prescriptions in her name as well as the names of Medicaid recipients."**
- **Office of Inspector General, Health and Human Service, Criminal Actions (Sept. 2005), http://oig.hhs.gov/fraud/enforcement/criminal/05/0905.html, reported on World Privacy Forum.**

Medical Identity Theft

- **A Pennsylvania man discovered that an imposter used his identity at five different hospitals to receive more than $100,000 worth of medical treatment. At each hospital, the imposter created medical histories in the victim's name.**
- United States v. Sullivan, Affidavit of Probable Cause for Arrest Warrant. Also "AG Corbett announces arrest of Philadelphia man in $144,000 identity theft scam," Press Release, July 29, 2005, reported on World Privacy Forum.

Medical Identity Theft

- **In another case, a Missouri identity thief used multiple victims' information to establish false drivers' licenses in their names. The thief entered a regional health center, acquired the health record of the victim she was impersonating at the time, and intentionally altered the records in order to obtain a prescription in the victim's name.**
- United States v. Sample, 213 F. 3d 1029, 2000 U.S. App. Lexis 11945. (8th Cir. 2000), reported on World Privacy Forum.

Medical Identity Theft

- **Victims in Southern California were given medical tests by non-physicians and had false diagnoses inserted into their medical files by a network of medical imaging companies.**
- **The individuals actively recruited Medicare beneficiaries with the promise of free transportation, food, and medical care.**
- **Posing as doctors and health professionals, they obtained the victim's personal information and photocopied the victim's Medicare cards. The operation raked in $909,000 using victims' personal and insurance information.**
- United States v. Dzugha, Case No. 5:05-cr-00589-JF, Indictment at 4-7 (N. Cal), reported on World Privacy Forum

Medical Identity Theft

- **The University of Connecticut Health Center, concerned after a case of medical identity theft occurred there, began checking patient driver's licenses. Staff at the health center told researchers that approximately a dozen people each week attempted to impersonate beneficiaries. Health center staff was concerned about the health dangers of false entries in medical records arising from medical identity theft.** **World Privacy Forum**

Physician Identity Theft

- **A physician's social security number, driver's license, and other identification numbers were in her file so she could be credentialed to practice in a multidisciplinary pain treatment program.**
- **Then someone posed as her to open utility accounts and get a credit card, racking up $5,000 in bills. An employee, since fired, used information in the credentials file to steal the anesthesiologist's identity.**
- **Six years later, she is still dealing with the fallout.**
- AMANews, Safeguarding identity: Tips to stave off a growing problem, June 26, 2006, http://www.ama-assn.org/amednews/site/free/bisa0626.htm

The Incidence of Identity Theft

How Bad Is It ?

Incidence and Cost

- **FTC 9/3/03 Survey of**

  Identity Theft Shows 27.3 Million U.S. Victims in Past 5 Years
- **Last year's identity theft losses to businesses and financial institutions totaled nearly $48 billion and**
- **consumer victims reported $5 billion in out-of-pocket expenses.**

Cost

“A billion here, a billion there, and pretty soon you're talking real money"

Everett Dirkson

(alleged remark)

Incidence

- **Identity theft remains the #1 concern among consumers contacting the Federal Trade Commission.**
- **According to 2 studies done in July 2003 (Gartner Research and Harris Interactive), approximately 7 million people became victims of identity theft in the prior 12 months.**

- **That equals 19,178 per day,**
  799 per hour,
  13.3 per minute.

Source

- 20% of all cases involve telecommunications and the Internet (FTC)
- Identity theft also occurs from:
  - Dumpster diving
  - Mail theft
  - Interception cell phones, email
  - Social engineering
  - Employee theft

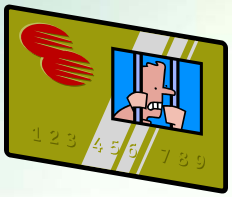
The Top Ten States

Top 10 locations in # of victims

1. **Washington D.C.**
2. **California**
3. **Arizona**
4. **Nevada**
5. **Texas**
6. **Florida**
7. **New York**
8. **Washington**
9. **Maryland**
10. **Oregon**

The 2002 FTC Annual Report (www.consumer.gov/sentinel)

Victim Impact



Victims now spend an average of 600 hours recovering from this crime, often over a period of years.

Even after the thief stops using the information, victims struggle with the impact of identity theft:

- **increased insurance or credit card fees,**
- **inability to find a job,**
- **higher interest rates and**
- **battling collection agencies and issuers who refuse to clear records despite substantiating evidence of the crime.**

Source: Federal Trade Commission

Finding Out

Approximately 85% of victims found out about the crime due to an adverse situation - denied credit or employment, notification by police or collection agencies, receipt of credit cards or bills never ordered, etc.

Only 15% found out through a positive action taken by a business group.

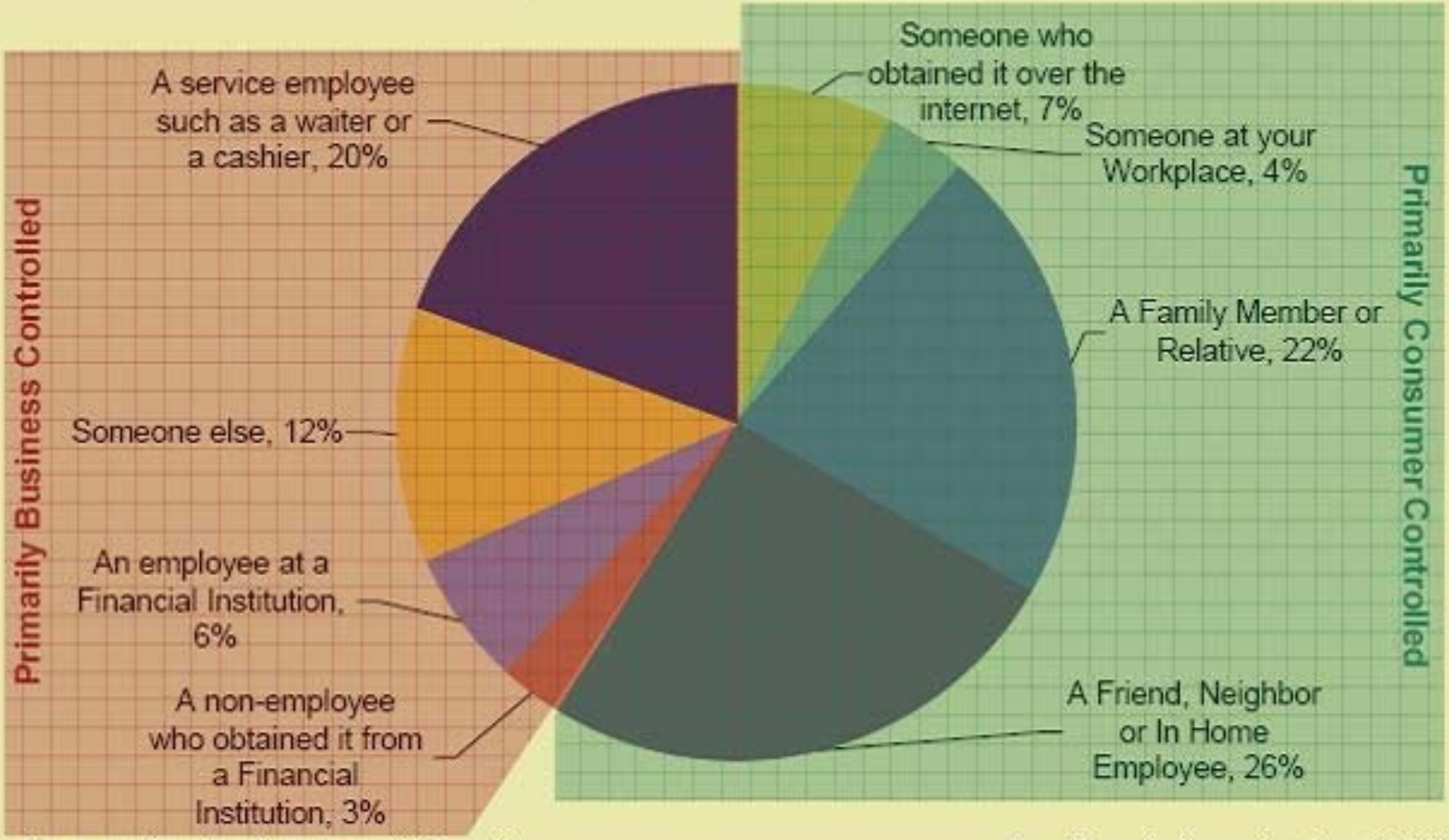
Source: Federal Trade Commission

Used with permission.

JAVELIN STRATEGY & RESEARCH

59% of Fraud Operators are Someone Close to Victim

From the 36% who know "Who"



n = 183

Q26: Was the person who misused your personal information...

Base: Those who knew who misused their information

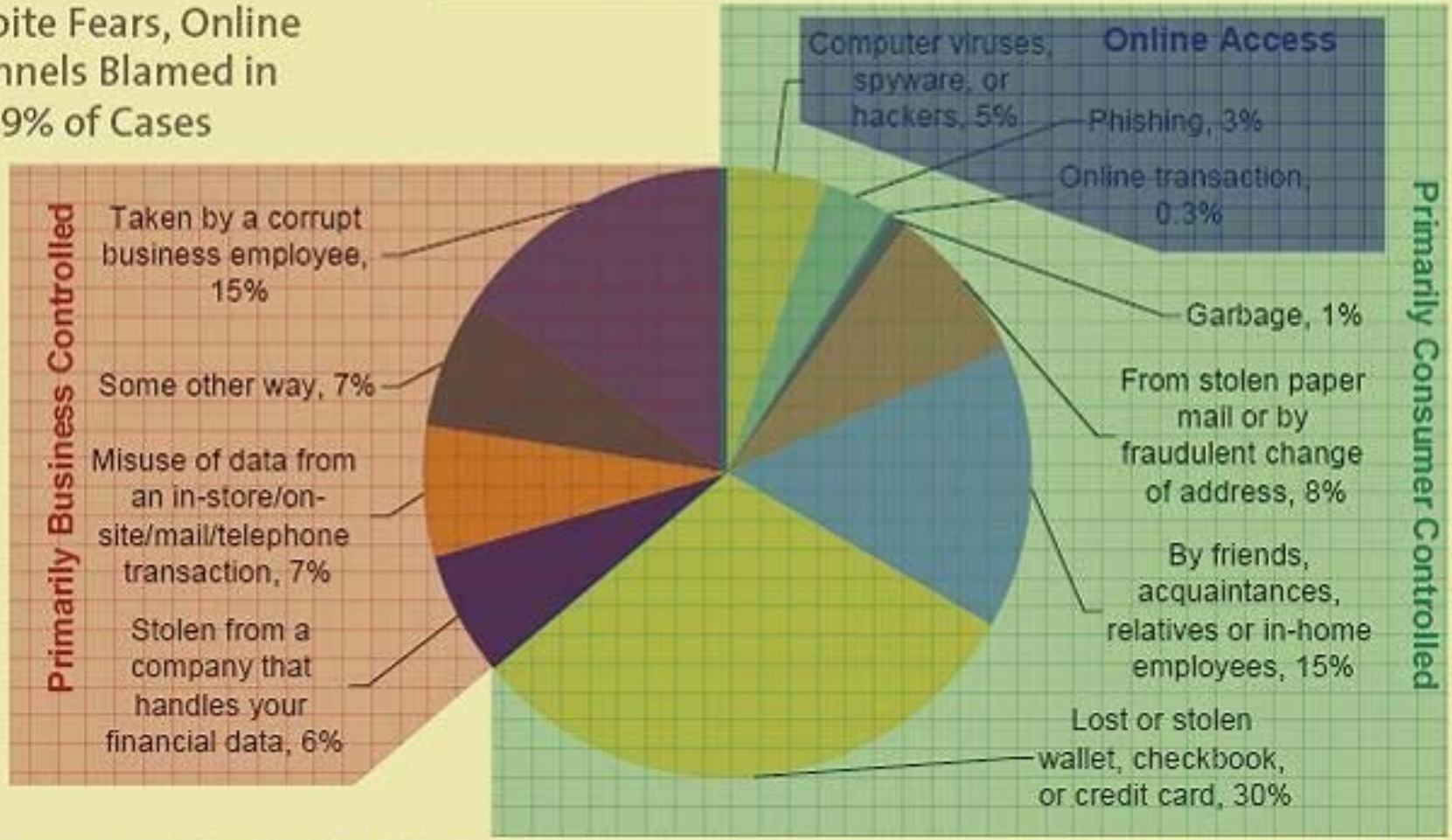
Used with permission.

JAVELIN STRATEGY & RESEARCH

Consumers in Primary Control in 63% of Theft Cases

From the 47% who know "How"

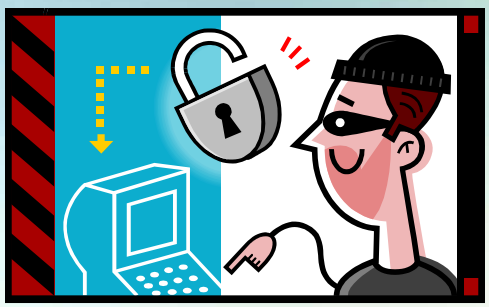
Despite Fears, Online Channels Blamed in Just 9% of Cases



n = 235

Q29: How was your personal information obtained? Was it...

Base: Those who knew how their information was obtained



The 12 Most Important

HIPAA Security Steps to Prevent or Mitigate The Risk of Identity Theft

Identity Theft and Health Care Providers

- **HIPAA Security is more important than ever, but the tools to fully implement industry standards are not always fully available; and when available, may not be fully implemented due to system compatibility, access to IT personnel and/or cost constraints.**

Step 1

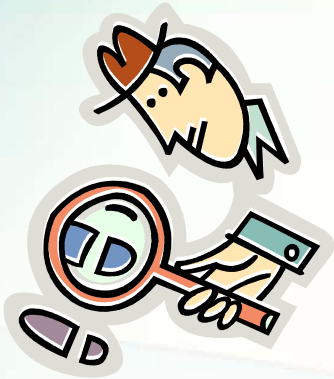
1 - Develop the Corporate Will to Prevent Identity Theft.

- ID theft in the news can bring home the importance of security.
- Obtain buy in from management to support identity theft prevention policies.

HIPAA Security Rule
45 CFR 164.306 Security Standards

- General requirements. Covered entities must do the following:
- (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- (3) Protect against any reasonably anticipated uses or disclosures of such information …
- (4) Ensure compliance … by its workforce.

Step 2



2 - Audit trails.

not all legacy systems provide the ability to track who accesses each record, and yet this can be one of the most important tools in determining who the perpetrator of identity theft may be.

You may want to assess the feasibility of “front door” software controls or upgrades with tracking abilities.

HIPAA Security Rule
45 CFR 164.312 Technical Safeguards

- ***Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).**
- ***Implementation specifications*: *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.**
- ***Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.**

HIPAA Security Rule
45 CFR 164.308 Administrative Safeguards

- **(a)(1)(ii)(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.**

National Institute of Standards and Technology

- **The NIST Standards cited in the final Security Rule in reference to access controls are more exacting than HIPAA:**
- Special Publication 800–14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*
- NIST Special Publication 800–33, *Underlying Technical Models for Information Technology Security*.
- **For example, NIST guidance includes an "audit trail" that tracks exactly what each user touches and modifies, but a specific audit trail requirement is not in the HIPAA final rule.**

Step 3

- **3 – Analyze Risk – Avoid Surprises**
- **Educate staff and managers so they alert the Security Officer to business plans that add websites, vendor links, and new places to store and access EPHI.**
- **Make sure a requirement for a risk assessment is a preliminary step to new ventures involving EPHI.**

HIPAA Security Rule
45 CFR 164.308 Administrative Safeguards

(a)(1)(ii)(A) *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information

- **(B) *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level…**

Step 4

4 – Enforce “Need to Know” rules that limit access to sensitive patient records.

- **“Just because someone works for the covered entity does not necessarily mean they [are entitled to] look at patient records,"**
  Edward Meyers, HIPAA chief security officer for the Missouri Department of Mental Health, quoted in HIPAA Compliance Strategies, Report on Patient Privacy, June 2005.
- **Common or shared User IDs and passwords are not permitted.**
- **Define role-based access requirements for employees, temps, students, and volunteers**
- **Plan how to manage access for jobs that can overlap across departments and shift duties.**

HIPAA Security Rule
45 CFR 164.308 Administrative Safeguards

(a)(3)(i) Standard. Workforce Security.

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information…, and to prevent those workforce members who do not have access … from obtaining access to electronic protected health information.

(ii) *Implementation specifications:*

(A) *Authorization and/or supervision* (Addressable).

(B) *Workforce clearance procedure* (Addressable).

HIPAA Security Rule
45 CFR 164.308(a)

- **(3)(ii)(C)** ***Termination procedures*** **(Addressable).**
- **(4)(ii)(C)** ***Access establishment and modification*** **(Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.**

- **JCAHO IM.2.20** Policies and procedures address security procedures that allow only authorized staff to gain access to data and information.

Step 5

- **5 – Authentication persons and entities accessing or modifying records**
- **Business may want connection in advance of adequate authentication controls.**
- **Entities may want to connect referral sources, business partners, and allow the support staff of outside physicians to do preparation work prior to seeing a patient.**
- **Data integrity can be at risk when uncredentialed outside support staff begin to modify the legal medical record.**

HIPAA Security Rule
45 CFR 164.312 Technical Safeguard

- **(d) *Standard: Person or entity authentication.* Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.**

Step 6

6 - Physical Security – lock it up!

- Managers and staff should be on the look out for unsecured records and suspicious persons
- Don’t leave records in patient accessible door pockets
- Lock physician offices when possible
- Have security patrol for computers left logged in
- Have security watch for misplaced garbage that may contain PHI

HIPAA Security Rule
45 CFR 164.310 Physical Safeguards

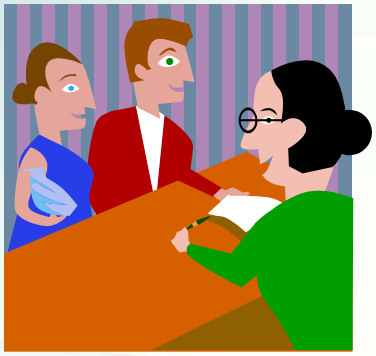
- ***(a)(1) Facility access controls.*** **Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.**

- **(2) *Implementation specifications: . . .***
- **(iii) *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.**

Step 7

- **7 - Limit reliance on SSNs**
- **“There's no reason a patient's Social Security number should be on a chart hanging off the front of a hospital bed, or on a wristband.”** Source, Bob Sullivan, Hospital ID theft: How to protect yourself, 12/23/05 http://redtape.msnbc.com/2005/12/hospital_id_the.html
- **“The biggest vulnerability of hospital patients is that their Social Security numbers often double as a medical identifier. For identity thieves, ‘Social Security numbers are the key to the golden kingdom…’"** Wednesday, By Kevin Helliker, WSJ's Health Journal: “Identity thieves find ways to target patients,”The Wall Street Journal, February 23, 2005 quoting Mari Frank, a California attorney specializing in identity theft.”

Step 8

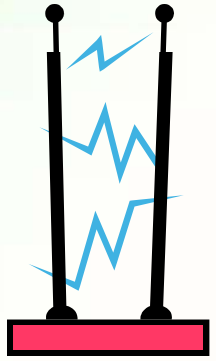


- **8 – Ask for Patient Identification -**
- **Some providers at Kaiser Permanente, a health network with 30 medical centers and 431 medical offices, now ask to see a driver's license in addition to the program's health card.**

Step 9

- **9 – Control Wireless Use – Although your medical center may have created secure lines and email systems behind the system firewall, you may have providers and managers with home wireless computers performing work at home.**

Wireless Security



- **Wireless networking uses radio frequency signals to connect your computer.**
- **The amount of non secure wireless access points is alarming – a recent study showed how over 90% of Access Points have little or no security enabled.** Andrew Tabona, An Overview of Wireless Network Security, Windowsnetworking.com, Aug 8, 2005.
- **Michael Stokes, chief security officer for wireless technology company CD/Help, recently came across a Northern California health care provider that used wireless connections throughout its facility and, because of the lack of security, broadcast patients' medical data indiscriminately.**
- Bob Lemos, Wireless Minefield, CNET News.com, July 1, 2002
- http://news.com.com/Insecure+networks+could+lead+to+lawsuits/2009-1033_3-940460.html

HIPAA Security Rule
45 CFR 164.312 Technical Safeguards

(a)(1) Standard: Access Control. (2) Implementation Specifications:

(iv) *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

(e)(1) *Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) *Implementation specifications:*

(ii) *Encryption* (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Step 10

10 - Control your vendors

Today there are many forms of hospital vendors, e.g., Transcriptionists, IT specialists, coders, record retention companies and disaster recovery companies that may access electronic health records by a variety of electronic means: email, T-1 lines, VPNs, or dial ups.

Conduct a security assessment and obtain contractual protections before providing a hook up. Also, consider isolating the access.

"An audit finds that the biggest risk of data breach or theft comes from careless employees or consultants who don't properly secure the data they are entrusted with."

- Martin H. Bosworth, ConsumerAffairs.Com, June 28, 2006

HIPAA Security Rule
45 CFR 164.314 Organizational Requirements

- **(b)(1) *Standard: Business associate contracts and other arrangements.* A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.**

Step 11

11 - Shred it (paper, disks, CDs, media) and have a plan to “sanitize” hard drives

- **When you delete a file, your computer does not destroy the file contents from the disk - it only deletes some "references" on the file from some system tables.**
- **The contents remain on the disk until another file overwrites.**
- **Any software recovery tool can restore the data if it hasn't been overwritten or thoroughly erased.**

HIPAA Security Rule
45 CFR 164.310 Physical Safeguards

- (d)(1) ***Standard: Device and media controls.*** **Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.**
- **(2) *Implementation specifications:***
  - **(i) *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.**
  - **(ii) *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.**
  - **(iii) *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore. . .**

Step 12

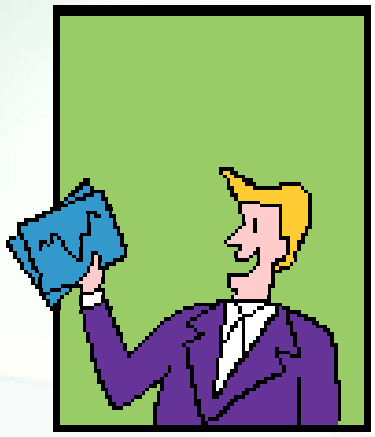
- **12 – Train Staff**
- **If staff are told the risks and receive training that helps them understand the application of privacy and security in their area, they will be the greatest source of protection for you and your patients.**

HIPAA Security Rule
45 CFR 164.308 Administrative Safeguards

- ***(a)(5)(i) Standard: Security awareness and training.***
- **Implement a security awareness and training program for all members of its workforce (including management).**
- ***(ii) Implementation specifications.*** **Implement:**
- ***(A) Security reminders*** **(Addressable). Periodic security updates.**

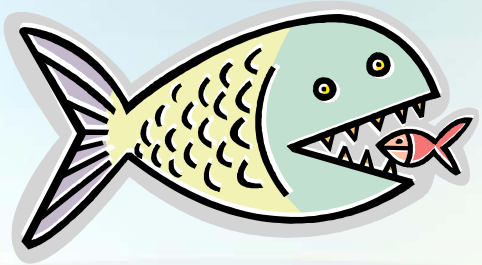
Social Engineering

The Con



- A reputable source (supposedly)
- Creates fear and sense of urgency
- Creates a strong desire to respond:
  - Offer of a gift or financial benefit
  - Access to a great job
  - Threat of government or legal action if you don't respond immediately (FBI or jury duty)
- All require you to send back, or go to a website and enter, your private information

Pfishing or Phishing



- **Pfishing is designed to steal identity by tricking the recipient into disclosing valuable personal data—like credit card numbers, SSN, passwords, account data, or other information.**
- **Schemes can be carried out in person or over the phone or online through spam e-mail or pop-up windows.**
- **Pfishers pretend to be your bank, the govt, a local court demanding jury duty, or even your bank, or credit company trying to validate your account or verify suspicious activity.**

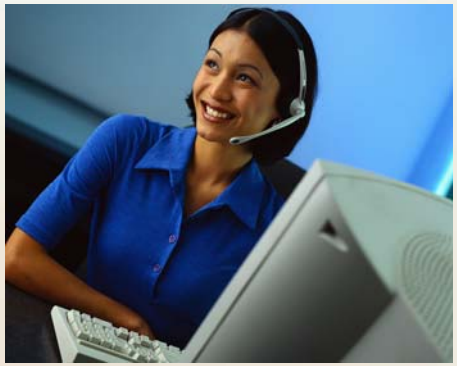
Social Engineering

- **Job scams – offer of a part time job to accept checks or orders into your own account and then forward the money electronically.**
- **Visa/Mastercard – employee trying to confirm unusual activity on your account and asks for the code on back of your card.**
- **Pfishers purchase look-alike web site names, or names of the legitimate company with extensions, like legitimate company name + “accounts,” or +“verification.”**

Source: http://www.idtheftcenter.org/alerts.shtml

Social Engineering

- **Lottery winner – you have won a lottery you did not enter.**
- **Free Credit Report - almost all these emails are scams.**
- **Do not call lists – scammers offer to put persons on federal do not call lists and request SSN**
- **Electronic resume requested for jobs that require SSN or date of birth.**
- **Telephone calls from charities asking for donations by credit card.**



Source: http://www.idtheftcenter.org/alerts.shtml

Hospital Personnel

- **(first reported Dec 2002)**
- **Scam artists may pose as a hospital employee asking patients to either verify their information or help fill in some blanks.**
- **They may carry clipboards or wear hospital lab coats.**
- **Hospital personnel should be on the lookout for these persons and require identification.**

Source: http://www.idtheftcenter.org/alerts.shtml

Social Engineering

- **If you think you have been scammed, do not respond to the email. Do not send a “do not contact me again” message.**
- **Forward it to itrc@idtheftcenter.org Or FTC at 877-FTC HELP spam@uce.gov**

Legal Protections

Rights, Responsibilities

And Self-Help

The Enforcers

- **Federal Trade Commission**
  - **In 1998, Congress gave the FTC responsibility to establish and maintain a repository of identity theft complaints and to provide victim assistance and consumer education.**
  - **The agency also has brought enforcement actions against companies that failed to take appropriate precautions against security lapses.** http://www.ftc.gov/opa/2003/04/idttestimony.htm
- **Department of Justice prosecutes crimes.**
- **Local police investigate crimes.**
- **State Attorney Generals protect consumers and enforce state laws.**
- **Federal Bureau of Investigation investigates interstate crimes.**
- **Secret Service After 9/11 responsibility for credit card crimes was transferred from the FBI to the Secret Service. They have a limit of $2,000 before investigating a crime.**
- **U.S. Postal Service investigates identity theft when your mail is involved.**

Self Help for ID Theft

1. **Place a fraud alert on your credit reports, and review your credit reports.**

- **Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two.**
  - **Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374- 0241**
  - **Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013**
  - **TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790**
- **Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your SSN will appear on your credit reports**

Self Help for ID Theft

2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

- **Call and speak with someone in the security or fraud department of each company. *It's important to notify credit card companies and banks in writing.* Send your letters by certified mail, return receipt requested, so you can document what the company received and when.**
- **When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number.**
- **If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the forms to dispute those transactions.**

Self Help for ID Theft

3. File a report with your local police or the police in the community where the identity theft took place.

- **Get a copy of the police report or at the very least, the number of the report. It can help you deal with creditors who need proof of the crime.**

4. File a complaint with the Federal Trade Commission.

- **The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.**
- **You can file a complaint online at www.consumer.gov/idtheft.**

Self Help for Lost or Stolen Credit Cards

5. **If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on how quickly you report the loss.**
   - **If you report the loss or theft within two business days of discovery, your losses are limited to $50.**
   - **If you report the loss or theft after two business days, but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to $500 of what the thief withdraws.**
   - **If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account after the end of the 60 days.**
- **Note: VISA and MasterCard voluntarily agreed to limit consumers' liability for unauthorized use of their debit cards in most instances to $50 per card, no matter how much time has elapsed since the discovery of the loss or theft of the card.**

Credit Monitoring Services

Services may differ

Some may offer:

- **Unlimited access to one or all three of your credit reports and credit scores.**
- **Notification within 24 hours of critical changes to one or all 3 reports.**
- **May include up to $25,000 ID theft insurance.**
- **May cost up to $15-$25 month.**
- **Use caution in selecting a service: know what you are getting for your $ and check with the BBB.**

ID Theft Insurance

Identity-theft insurance.

- **Farmers Group, American International Group (AIG), Travelers, Chubb, Encompass, and some credit-card issuers offer these policies. They usually cost $25 to $50 per year, and have a maximum benefit of $15,000 to $25,000 and deductibles of $100 to $250.**
- **Policies generally cover the expenses of cleaning up the crime, including attorney's fees, costs of mailing correspondence, and lost wages. They seldom cover the out-of-pocket loss to the victim, typically about $800.**
- ConsumerReports.org, ID-theft protection services typically not worth the money, October 2003

Firewalls

- **Preventing a virus infection on your computer is not enough!**
- **Spyware, adware and malware that can get onto your computer through an open port.**
- **Protection means installing and updating a firewall and/or specific programs to block spyware.**
- **You can also use Encryption to lock your computer files and folders.**

ITADA

- **The Identity Theft and Assumption Deterrence Act ("ITADA") 28 U.S.C. §1028 (2000).**
  - **ITADA was the first comprehensive effort to rewrite the federal criminal code to address the effects of identity theft on individuals.**
  - **ITADA defines identity theft as a crime, recognizes the consumer as the victim, and provides for specific remedies and penalties.**
  - **ITADA directs the Federal Trade Commission to establish a centralized clearinghouse "to record and track complaints, and to provide consumer education service for victims of identity theft."**

Fair Credit Reporting Act
15 U.S.C. § 1681 et seq.

- You must be told if information in your file has been used against you.
- You can find out what is in your file
- You can dispute inaccurate information
- Incorrect information must be corrected
- You can dispute inaccurate info with the source
- Outdated information must be removed
- Access to your files is limited
- Your consent is required for certain disclosures
- You may ask to exclude your name from outside offers based on your credit score
- You may seek damages from violators
- http://www.ftc.gov/os/statutes/031224fcra.pdf

FACTA

- **The Fair and Accurate Credit Transaction Act of 2003 (FACTA) added new sections to the federal Fair Credit Reporting Act (FCRA, 15 U.S.C. 1681 et seq.), intended primarily to help consumers fight identity theft.**
- **FACTA gives victims of ID theft the right to contact a credit reporting agency to flag their account.**
  - **To place a fraud alert, you must provide proof of your identity to the credit bureau.**
  - **The fraud alert is initially effective for 90 days, but may be extended at your request for seven years when you provide a police report to the credit bureaus that indicates you are a victim of identity theft.**

FACTA

- **FACTA creates a new kind of alert, an active duty alert, that allows active duty military personnel to place a notation on their credit report as a way to alert potential creditors to possible fraud.**
  - **While on duty outside the country, military members are particularly vulnerable to identity theft. An active duty alert is maintained in the file for at least 12 months.**

Fraud Alert

- **If a fraud alert or active duty alert is placed on your credit report, any business that is asked to extend credit to you must contact you at a telephone number you provide or take other "reasonable steps" to see that the credit application was not made by an identity thief.**

FACTA

- **FACTA gives you the right to a free copy of your credit report <u>when you place a fraud alert</u>.**
  - **With the extended alert (seven years), you are entitled to two free copies of your report during the 12-month period after you place the alert.**
- **New FACTA provisions also allow you to "block" certain items on your credit report that resulted from identity theft.**

FACTA Limits on Medical Info

- **FACTA restricts credit reporting agencies from reporting medical information that will be used for employment, credit transactions or insurance transactions unless the consumer consents to such disclosures.**
- **The consent must be (a) in writing, (b) specific and (c) descriptive of the use for which the agency is disclosing the information (except for an insurance transaction).**
- **Additionally, creditor reporting agencies are prohibited from disclosing the name, address and telephone number of the medical furnisher (e.g. the hospital) responsible for specific information in the report.**
- **Creditors are disallowed from using consumer medical information in deciding whether to grant, or to continue granting, credit to a consumer.**
- **Regulations are still in proposed form. See 69 Fed. Reg. 23379-23407 (April 28, 2004).**

Free Credit Reports

- **The law also allows consumers to obtain a free copy of their credit report annually from each of the "big three":**
- **The only way to get your free reports is through a centralized source, a combined effort by the three national bureaus. Free reports are available through a dedicated web site, www.annualcreditreport.com.**
- **You may order by telephone at (877) 322-8228 or by mail.**
- **69 Fed. Reg. 35467-35501 (June 24, 2004)**

State Law

- **State laws in seven states enable individuals to obtain free credit reports annually in addition to the reports you can obtain under the federal law. If you live in the following states, take advantage of your ability to get an additional set of free reports each year: CO, GA, ME, MA, MD, NJ, and VT.**
- **Further, you may be able to receive a free copy if you have recently been denied credit, are a victim of fraud, are unemployed, or receive welfare benefits.**
- **Certain states have aggressively pursued identity theft laws.**

Other Reports

Call (800) 428-9623. Online: www.consumerdebit.com

- **ChexSystems (bank account history) Understand why you were denied an account at a financial Institution where Chex Systems, Inc was used in the decision process.**
- **SCAN Report (Shared Check Authorization Network), is a database of information that SCANSM Members use to help make check acceptance decisions or account opening decisions.**
- **Understand why you were denied check writing privileges or had difficulty opening an account where SCAN was used in the decision process.**

Other Reports

- **Contact Choicetrust.com for the following:**
- **The C.L.U.E.® Personal Property Report**
  - **provides a five year history of losses associated with an individual and his/her personal property.**
- **Employment History Report**
  - **contains information related to your employment history as well as other information regarding your background.**
- **Tenant History Report**
  - **contains information related to your tenant history as well as other information regarding your background**

Medical Information Bureau

- **Find out if information about your medical history is stored in the insurance industry data base, the Medical Information Bureau (MIB).**
- **You may receive a free copy of your MIB report one a year: Phone: (866) 692-6901 (TTY (866) 346-3642 for hearing impaired)**
- **www.mib.com/html/request_your_record.html**
- **The report is also free if you have received a letter from an insurance company stating they used MIB information to make a negative decision about you.**
  - **If you have not applied for individually underwritten life, health, or disability insurance during the preceding seven year period, MIB will not have a record on you.**
  - **You will be asked to certify under penalty of perjury that the information you provided about yourself to request MIB disclosure is accurate, complete and you represent that you are the person that is requesting disclosure.**

The Opting Out Option

Opt Out of Credit Offers

- **To get your name off mailing lists for pre-approved offers of credit, notify the credit bureaus at the following number: (888) 5OPTOUT or (888) 567-8688.**
- **You can also opt out online at**

  https://www.optoutprescreen.com
- **EquiFax, Experian, TransUnion and Innovis. created Optoutprescreen.com so that consumers could send in requests for removal (opt out) from pre-approved credit card and insurance offers. You are also given the choice of opting out for five years or you can opt out of firm offers permanantly.**

Do Not Sell Lists

- To protect your financial privacy, tell financial companies that they may not sell or share your customer data with other companies.
- Federal law requires banks, credit card companies, insurance companies, and brokerage firms to send you a privacy notice each year.
- Companies that sell customer data to unaffiliated third parties must enable you to "opt out." The privacy notice, mailed to you each year, will provide either a form to fill out or a toll-free telephone number to call. If you do not remember receiving a privacy notice, ask your financial company(ies) to mail the form to you.

Opt Out of Offers

- **Look for ways to "opt out" of mailing lists to reduce "junk" mail.**
- **Many mail order firms, magazines and credit card companies now provide a box to check if you do not want your name, address, and shopping habits sold to or shared with other companies.**

No Direct Marketing Mail List

- **Participate in the Direct Marketing Association's Mail Preference Service (MPS) to be added to a list of people who do not want to receive mail from the major nationwide catalog and marketing companies. The MPS does not stop all junk mail. For other types of unwanted mail, deal with each mailer directly.**
- **Mail Preference Service, PO Box 643, Carmel, NY 10512. No charge to opt-out by mail. The DMA's Web site charges $5.00 to opt-out online, http://www.dmaconsumers.org/**

Do Not Call

- To limit calls from telemarketers to your home phone or cell phone, sign up for the national "Do Not Call" registry. Call the toll-free phone number (888) 382-1222 (TTY (866) 290-4236) or register online at www.donotcall.gov.
- Your phone number will stay on the registry for five years, or until you ask for your number to be removed from the list, or your phone number changes.
- You can renew every five years.
- Both inter- and intra-state telemarketers must update their lists each quarter with those who enroll in the registry.

Opt Out of Catalogs

- **Abacus compiles a cooperative data base of catalog and publishing companies' customers. To opt-out of the Abacus database, write to Abacus, P.O. Box 1478, Broomfield, CO 80038 or email optout@abacus-direct.com**
- **Include full name and current address (and previous address if you have recently moved).**

Junk Mail and Calls

- **The following activities often result in "junk" mail and telemarketing calls:**
  1. **Filling out warranty and product registration cards.**
  2. **Joining or donating money to clubs, organizations, charities. (Tell them in writing not to sell or exchange your name with other groups.)**
  3. **Subscribing to magazines, book clubs and music/CD clubs. (Tell them not to sell your name.)**
  4. **Listing your phone number & address in the phone book.**
  5. **Entering sweepstakes and other contests**

Internet Use

- **If you are an Internet user, do not send sensitive personal information (phone number, password, address, credit card number, SSN) by chat lines, e-mail, instant messages, forum postings, or in your online profile. Assume your messages are not private unless encrypted.**
- **Opt-out of the sharing of online cookie data with advertisers by contacting the Network Advertising Initiative.**
- **www.networkadvertising.org**

Technical Security

Standards and Guidance

ISO Standards

- **ISO 17799 is a code of practice for information security. It details hundreds of specific controls which may be applied to secure information and related assets. It comprises 115 pages organized over 15 major sections.**
- **ISO 27001 is a specification for an Information Security Management System, sometimes abbreviated to ISMS. It is the foundation for third party audit and certification. It comprises 34 pages over 8 major sections.**

SAS 70

- **Statement on Auditing Standards (SAS) No. 70, *Service Organizations,* is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).**
- **A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes.**
- **Service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.**

NIST

- **NIST Special Publication 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*.**
- **SP 800-69 provides guidance to home users, such as telecommuting employees, on improving the security of their home computers that run Windows XP Home Edition.**

- **NIST Special Publication 800-66 *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.***
- **This Special Publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule.**

Resources

- http://www.consumer.gov/idtheft/
- http://www.privacyrights.org/identity.htm
- http://www.consumer.gov/sentinel/
- http://www.idtheftcenter.org/
- http://www.usdoj.gov/criminal/fraud/idtheft.html
- http://csrc.nist.gov/
- http://www.knightsbridgecastle.com/
- http://usa.visa.com/personal/security/protect_yourself/id_theft/if_it_happens.html
- http://www.lavasoftusa.com/software/adaware/
- http://spywarebot.com/
- http://www.anonymizer.com/consumer
- http://www.llrx.com/features/idtheft.htm