Privacy Review for Pharmaceutical Vendors and Solution Providers

John Mack, MS, MPhil
VirSci Corporation
Publisher, *Pharma Privacy Watch*
www.virsci.com
johnmack@virsci.com
215-504-4164

Agenda

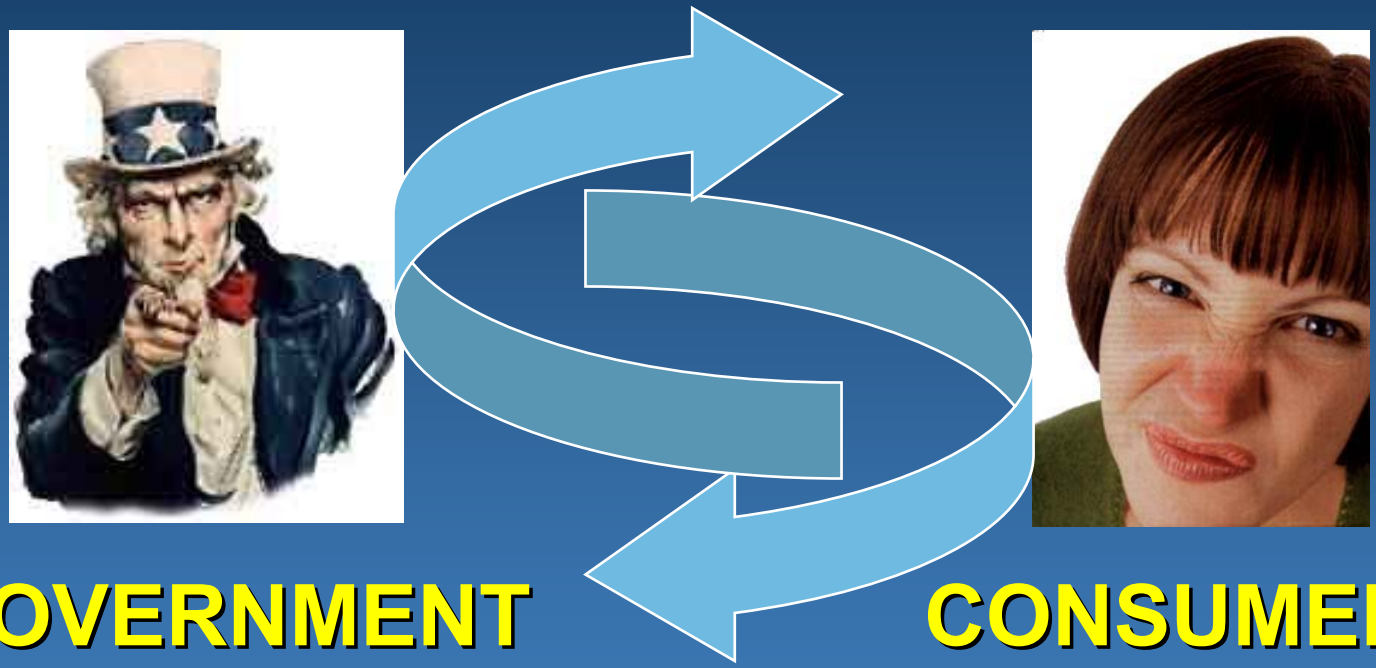
- FTC's Fair Information Practice Principles, COPPA and HIPAA
- Pharma Privacy Compliance with Fair Information Practice Principles (FIPs)
- Federal CAN-SPAM Law
- Selected State Law Synopses
- Privacy Self-Assessment for Vendors

Pharma companies and their agents collect sensitive personal information from consumers through several channels

- Health web sites
- Research
- Rebate programs
- Patient assistance programs
- Targeted marketing programs
- Market research (e.g., focus groups)
- Pharmacy compliance programs

Vendors often assist pharma companies to collect personal consumer data (PCD) or use PCD to carry out educational, marketing, or research programs for pharma clients who expect vendors to have best-in-class privacy and security policies and programs.

The more data you collect, the greater the odds that you will have problems with…



Consequently, pharma is under pressure to assure that their vendors and information handling partners are privacy certified as a condition for doing business with them. A critical privacy self-assessment is a necessary component of your certification process.

Privacy is a major concern, especially among "health seekers"…

- **Eighty-nine percent of health seekers on the Internet are concerned that a Web site might sell or give away information about what they did online.** (source: Pew Internet & American Life Project survey, 2000)
- **Only 14% of online health seekers have a "high level of trust" of Pharmaceutical company or product web sites.** (source: 2000 Cyber Dialogue survey commissioned by the Internet Healthcare Coalition and the California Healthcare Foundation)
- **Which translates into a profound lack of trust and government regulations.**

Pharma companies will increasingly look to vendors who can prove that they can be trusted with sensitive personal consumer information.

Fair Information Practice Principles (FIPs)

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Security/Integrity
- Chain of Trust/Onward Transfer
- Enforcement/Redress

HIPAA
What is it?

- Health Insurance Portability and Accountability Act of 1996
- Primary purpose is to improve health insurance accessibility for people changing employers or leaving workforce
- Also includes “Administrative Simplification” provisions to protect patient privacy and the security of electronic health data

HIPAA
Who is covered?

- **Covered Entity (CE)**
  - Certain health care providers
  - Health plans
  - Clearing houses
- **Business Associate (BA)**
  - Performs a function on behalf of a CE that involves the use or disclosure of individually identifiable health information
- **In general, pharmaceutical companies are not covered entities subject to HIPAA, but HIPAA is a national floor for medical privacy and is often used as a model for state medical privacy laws applicable to Pharmacos**

FIP: Personally Identifiable Information (PII)

- (a) a first and last name
- (b) a home or other physical address, including street name and name of city or town
- (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address
- (d) a telephone number
- (e) a social security number
- (f) an Internet Protocol ("IP") address or host name that identifies an individual consumer
- (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer
- (h) a facial image viewed in person or via digital or tape medium, or
- (i) any information that is combined with (a) through (h) above.

HIPAA
Protected Health Information (PHI)

- A subset of health information, including demographic information collected from an individual, and:
- (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

FIP: Notice/Awareness

Provide consumers clear and conspicuous notice of your information practices (What, Where, Who, When):

- what information you collect
- how you collect it (e.g., directly or through non-obvious means such as cookies)
- how you use it
- how you provide Choice, Access, and Security to consumers
- whether you disclose the information collected to other entities
- whether other entities are collecting information through your site

Question for vendors: What's the best way to notify consumers about your information collection and handling practices? Should you have a privacy policy on your Web site?

HIPAA: Notice of Privacy Practices

Covered entities must provide a “notice of privacy practice” to each patient describing his/her rights regarding protected health information

- Uses and disclosures of information
- Rights and choices

FIP: Choice/Consent

- Offer consumers choices [Opt In] as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Including:
  - internal secondary uses (such as marketing back to consumers) and
  - external secondary uses (such as disclosing data to other entities).

Question for vendors: Your client asks for demographic information about the consumers in your database. Have you obtained the necessary opt-ins?

HIPAA: Authorization

- Authorization from patient is required for use or disclosure of PHI for purposes other than Treatment, Payment, or Operations (TPO)
  - e.g., use of patient data for pharmaceutical marketing as in use of pharmacy data for direct mail advertising by pharmaco

Question for vendors: You are a vendor tasked with assembling patient focus groups for a pharma client. You want to find qualified candidates by solicitation of local physicians. Are you subject to HIPAA regulations? What is a best practice procedure for doing this?

FIP: Access/Participation

- Offer consumers reasonable access to the information collected about them, including a reasonable opportunity to
  - review information and
  - to correct inaccuracies or delete information.

Question for vendors: You have PCD in a database. What's the correct procedure for handling access to your database by consumers?

HIPAA: Access

- HIPAA gives patients the right to review their medical records and request modifications. However, physicians are not required to make corrections based on these requests

FIP: Security/Integrity

- Must take reasonable steps to protect the security of the information collected from consumers. (FTC)
- Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current. (EU Safe Harbor)

HIPAA: Security Rule

- Covers only electronic PHI
- Required vs. “Addressable”
- Administrative and technical security
- Identification and authorization
- Session controls
- Auditing
- Physical environment
- Training and awareness

FIP: Chain of Trust/Onward Transfer

- Entity may transfer information to a third party that is acting as an agent if …
  - the entity enters into a written agreement requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles. (EU Safe Harbor)

Question for vendors: You have several sub-contractors working for you on a pharma client project. Several of them handle PCD. Do you have the necessary provisions in your sub-contractor agreements/contracts to assure that they abide by your privacy and security policies? How should you verify this compliance?

HIPAA: Business Associate Contract

- A business associate of a covered entity performs a treatment, payment, or medical operations function on behalf of a covered entity and requires access to PHI
- CE may disclose PHI to a BA if there is a written contractual assurance that the BA will take proper measures to protect PHI
- CE must disclose the “minimum necessary” information for BA to do its job

FIP: Enforcement/Redress

- Enforcement approaches include
  - industry self-regulation
  - legislation that would create private remedies for consumers; and/or
  - regulatory schemes enforceable through civil and criminal sanctions.
- FTC enforcement under Section 5 of the FTC Act for unfair and deceptive trade practices. FTC can take action against web site operators who violate their own publicly posted privacy policies

Question for vendors: Can the FTC sue you for unfair business practices if you are working under contract with a pharma company to handle PCD?

The Lilly Consent Decree

- Lilly was the first major company to settle an online consumer privacy complaint with FTC
- Settlement announced January 18, 2002
- No immediate monetary penalties, but the company could be subject to fines should it violate the consent order in the future
- Provisions apply to Lilly's vendors as well
- Serves as a guide to any company interested in implementing an internal privacy compliance program and vendor certification program

“All Eli Lilly got was a slap on the wrist. Let's have some real enforcement.”

– Sen. Hollings, sponsor of “Online Personal Privacy Act”

HIPAA: Enforcement

- HHS Office of Civil Rights enforces Privacy Rule
- Investigates complaints and resolves complaints or sends on to DOJ
- Civil monetary penalties (OCR)
  - $100 per violation
  - Capped at $25,000 for each calendar year for each identical requirement
- Criminal Penalties (DOJ)
  - Up to $250,000 & 10 years

Pharma Online Privacy Policy Analysis

If privacy compliance is good business, how well is the pharmaceutical industry doing?

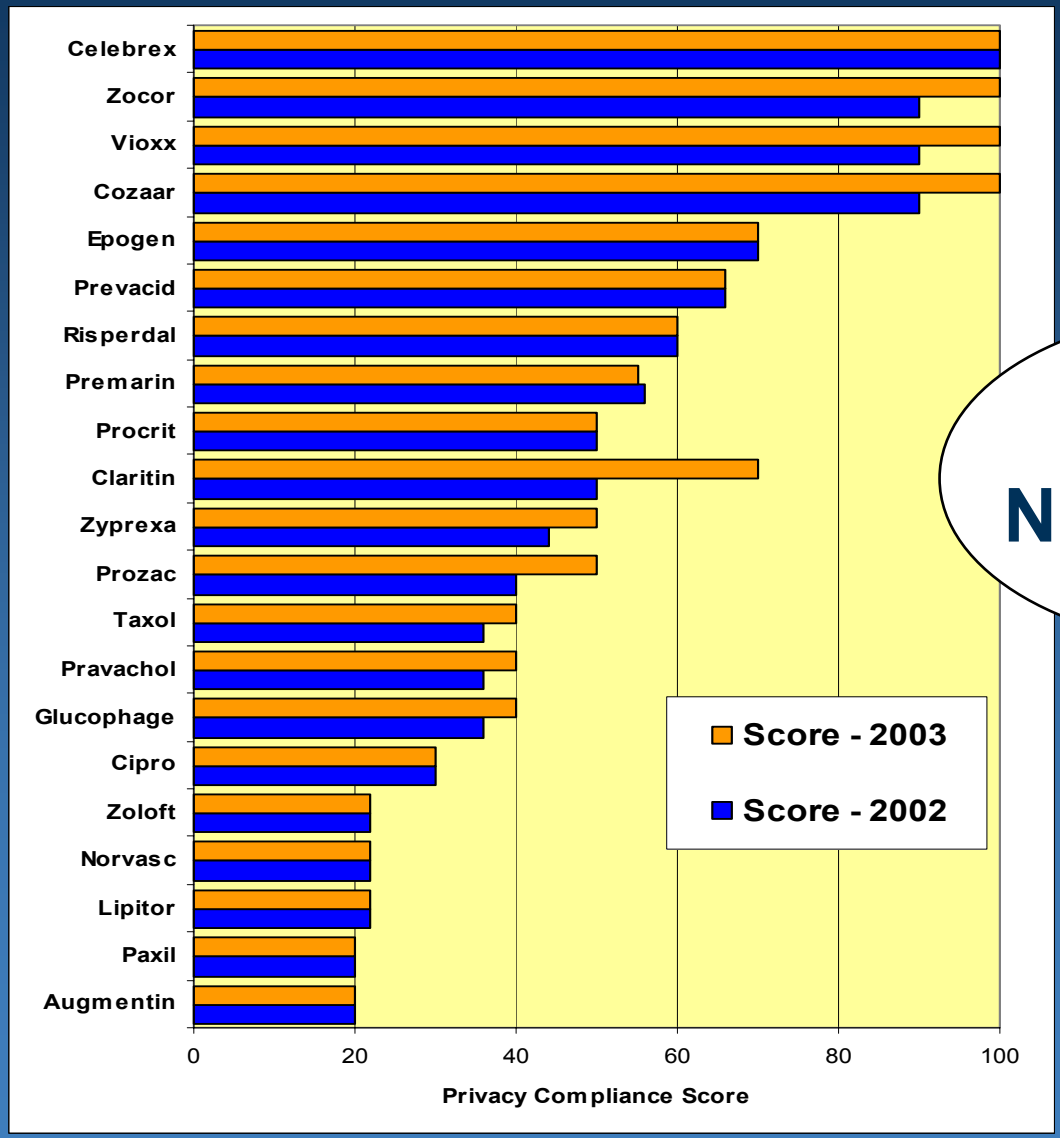
- Access the publicly available online privacy policies of the top selling Rx products
- Evaluate policy compliance with a select set of *Fair Information Practice Principles*
- Assign a numerical value of 20 for compliance with each principle and sum up to derive a "Privacy Compliance Score" (MAX=100)
- Rank products according to their Compliance Scores
- Compare to other healthcare industry entities

Privacy Compliance Score

Measurable Fair Information Practice Principles

- **Notice (20 points)**
  - Who is collecting info (4)
  - What info is collected (4)
  - When and how info is collected (4)
  - How info is used or disclosed to 3rd parties (4)
  - Whether or not visitors will be profiled (“cookie” policy) (4)
- **Choice (20 points)**
  - Right to opt-in or opt-out (10)
  - Right to limit disclosure to business partners, affiliates, and other 3rd parties (10)
- **Access (20 points)**
  - Ability to view info submitted voluntarily (10)
  - Ability to correct info (10)
- **Security (20 points)**
  - Security measures explained (10)
  - Different security measures for sensitive data (10)
- **Chain of Trust (20 points)**
  - Policy binding on business partners, advertisers, etc. (20)

Pharma Privacy Compliance Scores



AVERAGE = 51.4

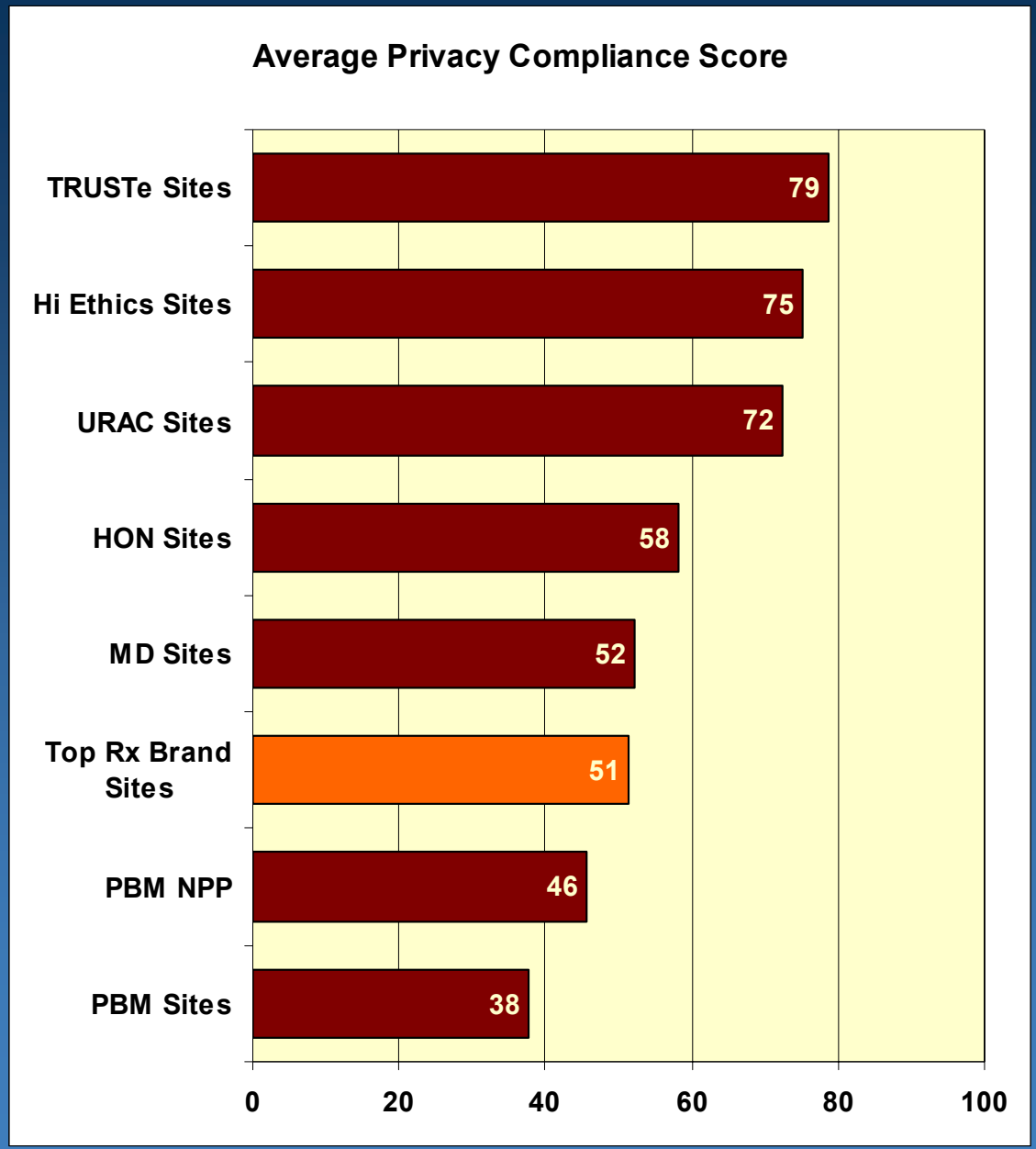
Oooh…
Not so good!

Benchmarking

- Pharma industry compliance scores are at the low end of the spectrum
- Industry self-regulatory programs work

Question for vendors:
How well does your privacy policy comply with fair information practice principles?

GET A FREE ANALYSIS



Children's Online Privacy Protection Act (COPPA)

- Requires parental consent to collect personal information online from children under the age of 13
- Applies if you "knowingly" collect personal information from children under 13
- Best practice dictates that for any attempt to restrict children under 13 (or 18) from entering personal information, the site should NOT use methods that could encourage age falsification

What's Wrong With This?

To improve our service to you, please provide us with some information about yourself. This information will not be used for any other purpose.

Name

Email Address

Street

City State Zip

Age

- 6-10
- 11-18
- 19-35
- 36-50
- 51-65
- 66+

Federal CAN-SPAM Act

- "Controlling the Assault of Non-Solicited Pornography and Marketing"
- Effective January 2004
- Some provisions may apply to all commercial e-mail, including permission-based, opt-in e-mail
  - B2B e-mail (e.g., e-detailing msgs)
  - One-to-one commercial e-mail (e.g., e-mail from sales rep to physician)
  - B2C e-mail (e.g., newsletters, product announcements, compliance messages, etc.)

Question for vendors: You manage an opt-in e-mail marketing newsletter for consumers for a pharma client. Is your program subject to CAN-SPAM? Are you liable for any violations of this law in relation to the program?

Some CAN-SPAM Act Provisions

- Opt-out must be honored within 10 business days
- Clearly identify e-mail as advertisement unless opt-in
- Bans use of deceptive subject lines
- Include valid postal address of “sender”
- ISPs and attorneys general can sue, not individuals

CAN-SPAM Act – Pharma Challenges

- Presents some challenges to Pharma, especially with regard to vendor-assisted e-mail marketing campaigns
  - Who is the "sender"?
  - Maintenance of Opt-out (suppression) lists
- Requires clarification from FTC
  - Define "primary purpose"
  - Use of identifiers in subject line (e.g., "ADV"). Not required if opt-in.
  - FTC will not implement a "do-not-spam" list

State Laws – Texas

- Texas Medical Privacy Act (SB 1136)
  - Effective January 1, 2004
  - Purpose: "to extend application of the federal privacy standards regarding marketing communications to anyone that comes into possession of protected health information, and to impose stricter standards related to certain product-specific communications that encourage a change in prescription drugs or prescription medical devices."

Question for vendors: Are you subject to this law?

SB 1136 (cont'd)

- Requires clear and unambiguous permission in written or electronic form to use or disclose protected health information for any marketing communication
  - e.g., making a product-specific written communication to a Texas consumer that encourages a change in products is considered marketing regardless of whether or not it can be justified as treatment or case management. Defines "product" as "a prescription drug or prescription medical device."

SB 1136 (cont'd)

- If using PHI to send marketing information by mail, envelope must not include certain information (e.g., medical condition)
- Requires removal of a person's name from a mailing list not later than the 45th day after the date request is received (was 5th day)

State Laws - California

- Online Privacy Protection Act (OPPA)
  - Affects every business that has a web site collecting information on-line
  - Operator "shall conspicuously post its privacy policy on the Web site“
  - Identify categories of information collected and entities with whom information is shared
  - State whether operator reserves right to change policy without notice
  - Operator must keep old versions of privacy policies and make them available on request up to five years

State Laws – California (cont'd)

- Security Breach Information Act (SB 1386)
  - Effective July 2003
  - Requires companies to disclose any security breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person
- Physician Prescribing Practices Act (AB 262)
  - Dead… for now
  - Would have established physician "do not call" list regarding use of prescribing data

Privacy Best Practices

- Have one consistent corporate privacy policy
  - helps to have a privacy officer to enforce across all brands
- Comply with Fair Information Practice Principles
  - develop and implement *practical* written procedures for the collection of and access to information
  - implement appropriate physical, technical, and administrative security measures
  - move towards EU Safe Harbor and/or HIPAA as best practice
- Make sure your information collection practices comply with your policy

Information Security Program

- Designate appropriate personnel to coordinate and oversee the program
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information
- Address these risks … whether performed by employees or agents, including:
  - management and training of personnel
  - information systems for the processing, storage, transmission, or disposal of personal information
  - prevention and response to attacks, intrusions, unauthorized access, or other information systems failures

Privacy Self Certification Assessment

- Do you have written Standard Operating Procedures (SOPs)?
  - Restrict access to PII to employees based on need
  - Restrict use of PII only for purposes allowed by data subject
  - Protect PII from external threats
  - Secure storage and transfer of PII
  - Subcontractors protect PII in equivalent manner
  - Train all employees, temporary workers, and subcontractors that have access to PII

Privacy Self Certification Assessment

- SOPs should cover all data collection methods
  - E-mail campaigns
  - Websites
  - BRCs
  - Mail or Call Center Inquiry
  - Coupon/Rebate Program
- Written procedures to handle opt-out requests from any source listed

Privacy Self Certification Assessment

- SOPs for secure access to PII
  - Segregate individuals who “use” PII from those who “administer” databases
  - Password control
  - Termination of access
  - Encryption
- Data Subject Access
  - How do you provide access? Via secure Web site? Phone? Mail?
  - How do you validate the identity of the person requesting access?

Privacy Self Certification Assessment

- Storage of hardcopies (e.g., BRCs, Faxes) of PII
  - Is your office secure at all times or only locked after hours?
  - Do you store documents containing PII in locked drawers or file cabinets?
  - What happens to hardcopies after PII entered into databases?

Privacy Self Certification Assessment

- Security of PII
  - Are databases containing PII secured behind a firewall?
  - Do you use intrusion detection software?
  - Do you monitor unauthorized *internal* access?
  - Do you have virus detection software in place and updated frequently?
  - Do you have an incident response SOP in place and are relevant employees trained on it?
  - How often do you perform a vulnerability assessment and how do you address findings?

Privacy Self Certification Assessment

- Other Questions
  - Do you have a Business Continuity Plan (BCPs)? e.g., off-site backup and recovery.
  - Do you perform quality assurance checks? i.e., How do you verify that communications to a data subject contain only information about that person and not any one else?
  - Do you allow temporary storage of PII by employees or contractors for use off-site? e.g., disks, etc.

Useful URLs

- VirSci Corporation
  - www.virsci.com
- Safe Harbor
  - http://www.export.gov/safeharbor/
- HIPAA
  - http://aspe.hhs.gov/admnsimp/Index.htm
- COPPA
  - http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm
- State Privacy Laws
  - http://www.epic.org/privacy/consumer/states.html

