Preparing for HIPAA: Compliance and Beyond

"Hot Button" Issues for Pharma

John Mack, MS, MPhil
President
VirSci Corporation
johnmack@virsci.com
215-504-4164

Privacy Issues are Everywhere
"Good privacy is good business"

- **New consumer privacy policies based on**
  - HIPAA
  - Gramm-Leach-Bliley
  - Internet notices
- **As HIPAA deadlines approach, media awareness increases**
  - forces all health-related companies to get a handle on how individual health information flows through their channels

Pharma NetTRUST HIPAA Issues Survey

- What are Pharma's "Hot Button" issues regarding HIPAA's privacy and security regulations?
- In-depth interviews of privacy officials, compliance officers, legal counsels, IT directors, and R&D professionals
- Follow-up quantitative survey of the industry – Pharmas and partners, including PBM's and HCO's

Does HIPAA apply to Pharma?

- **Are pharmaceutical companies "covered entities?"**
  - Provide treatment?
  - Transmit/maintain PHI?
- **Are they "business associates?"**
  - Performs or assists in the performance of…activity involving use of PHI on behalf of a CE?
  - e.g., diagnostic support
- **Are they "hybrid entities?"**
  - A *covered entity* whose covered functions are not its primary functions?
  - e.g., employee clinics

Pharma "Hot Button" Issues
Research

- **Patient recruitment**
  - Authorizations
  - Searching clinical databases for candidates
- **CRO, SMO knowledge and handling of issues**
- **Precedence - HIPAA? FDA? EU?**
  - **e.g., HIPAA vs. 21 CFR part 11**
    - E-signatures, security, audit trails, etc.
    - "giving IT fits"
- **De-identification issues**
  - Be sure that we "do not get individually identifiable patient information"

Pharma "Hot Button" Issues
Marketing

- **Must look into every "nook and cranny" of business to understand how we are collecting, using and sharing data"**
- **Be sure that we "do not get individually identifiable patient information"**
  - De-identification issues

Pharma "Hot Button" Issues
Sales

- **Impact on relationship with covered entity clients – especially hospitals and physicians**
  - Covered entities may deny access to pharma reps to prevent disclosure of PHI
- **Some CE's consider pharma to be business associates**

Pharma "Hot Button" Issues
Business Associate Contracts

- **Prevention of "unintended disclosure" of PHI is a responsibility of CE's**
  - Easier to get pharma to sign BA agreements than to implement HIPAA security standards to prevent disclosure of PHI – "unfair burden on Pharma"
- **Many pharmas feel that they are NOT BA's and should not sign contracts**
  - CE's need a "thorough understanding" about who is and who is not a BA

Pharma "Hot Button" Issues
Other Issues

- **Vendors**
  - Privacy is a "growth industry with lots of vendors in this space"
  - Inconsistencies in vendor interpretations of regulations
  - Vendors use scare tactics to increase business
  - Certification of vendors by HHS can help in evaluation of vendors
- **Management Buy-in**
  - Cost concerns, ROI
  - "Moving target" – waiting for final regs
- **Chief Privacy Officer**
  - "sine qua non" for pharma even though not required
  - "only way to get serious about privacy"

Pharma Online Privacy Policy Analysis

If privacy is good business and pharma companies need to get serious about privacy, how well are they prepared to adopt privacy best practices?

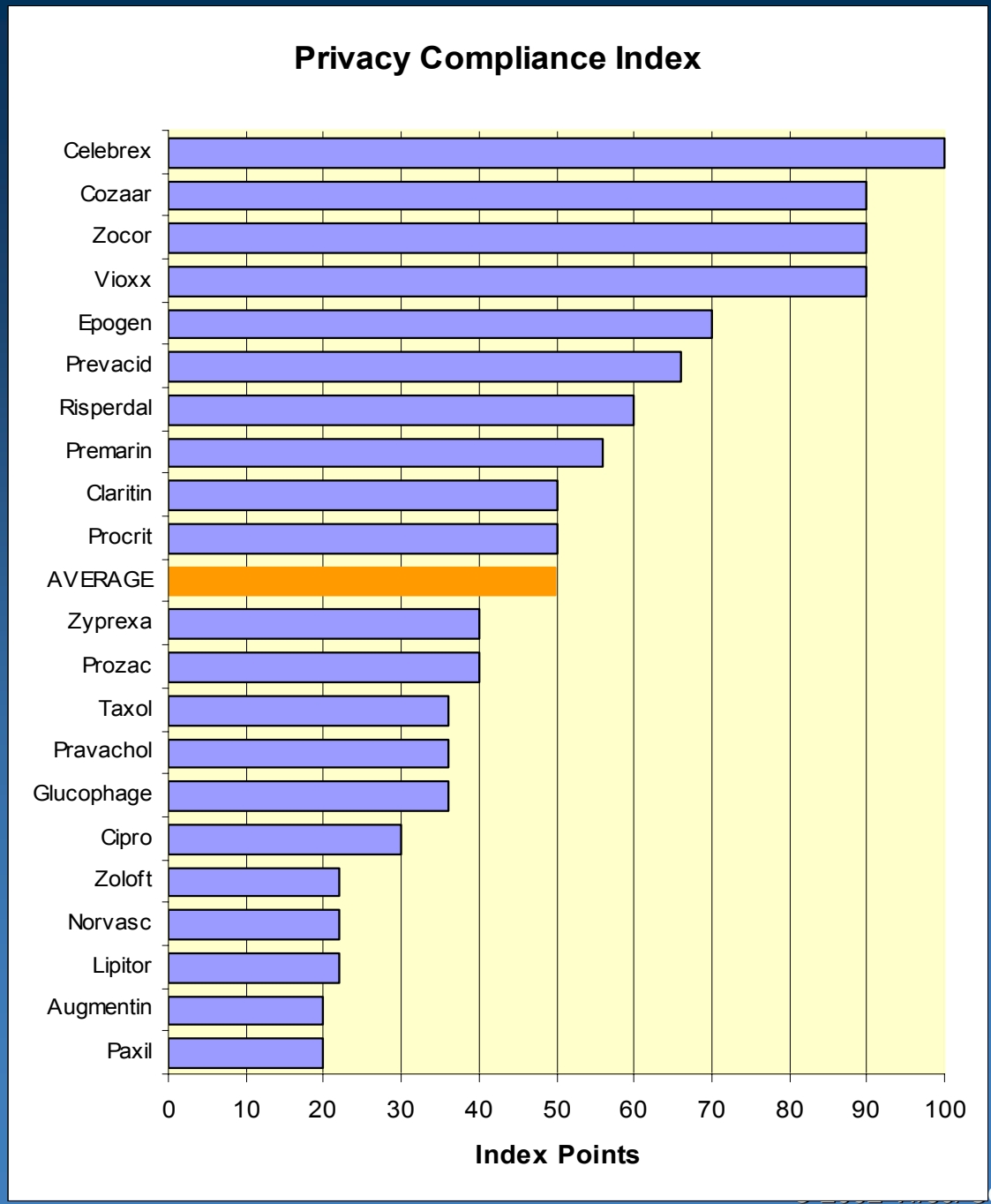
- **Access the publicly available online privacy policies of the top 20 or so Rx products**
- **Evaluate policy compliance with a select set of *Fair Information Practice Principles* (see next slide)**
- **Assign a numerical value of 20 for compliance with each principle and sum up to derive a "Privacy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

A Pharma NETtrust™ Study

Privacy Compliance Index Measures

- **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)

A Pharma NETtrust™ Study



Source:
Pharma NETtrust

Fair Information Practice Compliance Summary

Fair Information Practice Principle	Percent Full Compliance	Percent Partial Compliance	Percent Non-compliance
Notice	69%	31%	0%
Chain of Trust	46%	NA	54%
Access	31%	31%	38%
Security	31%	31%	38%
Choice	15%	54%	31%
ALL	8%	92%	0%

A Pharma NETtrust™ Study

Keep up on privacy laws and regulations

a periodic, pharmaceutical industry focused, e-telligent newsletter with up-to-date news about and analysis of privacy laws, regulations, and actions by Congress and federal agencies

- Pharma Federal & State Privacy Watch
  - www.virsci.com/FPW-hp.html
- HIPAA
  - http://aspe.hhs.gov/admnsimp/Index.htm