



Illinois Office of Health Information Technology



Fostering Public Trust in HIE & Protecting Patient Data

July 17, 2012

Illinois Health Information Exchange Authority
Data Security and Privacy Committee

John Saran, Summer Legal Associate, OHIT

Agenda

- ▶ 1. Illinois Privacy and Security Law Enforcement
- ▶ 2. Federal HIPAA Privacy and Security Rule Enforcement
- ▶ 3. Don't Mess with Texas
- ▶ 4. Proposals

Illinois Privacy and Security Laws Enforcement

Statute	Name	Penalty	Suit	Auth.
720 ILCS 5	Criminal Code of 1961: Identity Theft	Class 4+ felony	Y	AG/DA
410 ILCS 50/4	Illinois Medical Patient Rights Act	Petty Offense: \$1,000 Fine	N	AG/DA
210 ILCS 85/6.17	Hospital Licensing Act	Class A Misdem.	N	IDPH
225 ILCS 60/22	Medical Practice Act of 1987	Licensure to \$10,000 fine	N	IDFPR

Federal Privacy and Security Law Enforcement

- ▶ Department of Health Human Services, Office of Civil Rights (OCR) enforces HIPAA's Privacy and Security Rules
- ▶ OCR Reviews Complaints/Reports: (1) Administrative civil action or (2) DOJ criminal referral
- ▶ Between September 2009 and April 30, 2012:
 - 421 reports involving a breach of PHI for 500+
 - 57,000+ reports for under 500 individuals
 - Illinois is the 5th largest state in population.

Federal Privacy and Security Law Enforcement

▶ HIPAA's Civil Violations

Type	Penalty - 1 st Offense	Penalty - Identical Violations in Calendar Yr.
No Knowledge	\$100 – \$25,000	<\$1,500,000
Reasonable	\$1,000 – \$50,000	<\$1,500,000
Neglect – Corrected	\$10,000 – \$50,000	<\$1,500,000
Neglect – Not Corrected	\$50,000+	<\$1,500,000

Federal Privacy and Security Law Enforcement

▶ HIPAA's Criminal Violations

Type	Penalty	Imprisonment
Minimum	<\$50,000	<1 year
False Pretenses	<\$100,000	<5 years
Intent to Sell/Harm	<\$250,000	<10 years

Federal Privacy and Security Law Enforcement

- ▶ State Attorney General Authority
 - HITECH ACT → Bring civil actions against covered entities on behalf of state residents
 - Limit of \$100 per violation, up to \$25,000 in aggregate damages recovered for state resident
 - Requires permission from OCR to file

Don't Mess With Texas

- ▶ TX HB 300 Sharpens Enforcement – Effective September 1, 2012:
 - Consumer Website
 - Civil penalty range: \$5,000 to \$250,000 per violation
 - Cooperation with licensing agencies: revocation of license for a health professional = early retirement
 - Bounties for State Attorney Generals
 - Audits
 - Covered entity Certification of Policies
 - Required Breach Notification
 - Criminal Penalty Upgrade to Felony for PHI transfer with intent to harm or defraud.

Proposals

- ▶ (1) Monitoring
- ▶ (2) Enforcement Strategies
- ▶ (3) Breach Mitigation
- ▶ (4) Public Education

Monitoring

- Breach reporting rule
 - By breached entities upon discovery.
 - By public whistleblowers with some financial incentive
- Technical infrastructure within the HIE to allow for real-time network monitoring for privacy and security breaches
- Field audit teams.
 - HIE audits of participants.
 - Private third-party audits of participants.
 - User self-certification of audit

Enforcement Strategies

- **ILHIE Chief Privacy and Security Officer**
 - Oversee and manage all enforcement monitoring and audits
 - Manage budget for enforcement activities and incentives for inter-agency cooperation
 - Review all complaints actions against covered entities
 - Manage mitigation of breaches
 - Direct public education
- **Interagency Coordination**
 - State government enforcement of privacy breaches with the Attorney General, Office of Inspector General, Health and Family Services and County State Attorneys

Enforcement Strategies

- ▶ Civil and Criminal Tools:
 - **Civil:** Referral to licensing agencies responsible for taking disciplinary actions against each covered entity OR Department enforcing statutes with civil penalties.
 - **Criminal:** Sample increased state penalties
 - Class A Misdemeanor minimum, <\$25,000
 - Class 4 felony for neglect, \$25,000–\$50,000; (<1 yr)
 - [Federal: <\$50,000; <1 yr]
 - Class 3 felony for reckless disregard, \$50,000–\$75,000; (<2 yrs)
 - [Federal: <\$50,000; <1 yr]
 - Class 2 felony for fraud \$75,000–\$100,000; (3–5 yrs)
 - [Federal: <\$100,000; <5 yr]
 - Class 1 felony for sale/harm–\$100,000–\$250,000; (4–10 yrs)
 - [Federal: <\$250,000; (<10yrs)]

Breach Mitigation

- Corrective Action Plan requires the covered entity to (1) review, revise and maintain policies and procedures to be compliant with HIPAA Privacy and Security Rules; (2) conduct robust trainings of all staff
- Monitor who reports back to the ILHIE on the ongoing compliance efforts
- Biannual Reports
- Insurance or damage funds

Public Education

- Maintain a webpage focused on enforcement reporting results
- Quarterly semi-mandatory webinars on enforcement actions
- Solicitation of non-profit organizations for public education programs with grant money