

Re: Privacy Breach Enforcement Briefing Summary

I. Executive Summary

The Office of Health Information Technology (“OHIT”) submits this Briefing Summary to the ILHIE Authority Data Security and Privacy Committee to provide initial suggestions on the mechanisms that could be instituted to build public trust in the ILHIE’s protection of patient data privacy and security.¹

OHIT conducted a comprehensive review of Illinois law protecting the confidentiality of protected health information (“PHI”) and discovered great disparities between state enforcement mechanisms and the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)’s strong civil and criminal penalties for HIPAA’s Privacy and Security Rule violations. In fact, nearly all Illinois criminal violations had a maximum sentence of a Class A Misdemeanor, carrying a fine not exceeding \$2,500 and/or up to one year of imprisonment per violation. Very few of these statutes provided a civil right of action for the victim to recover damages to remedy harm suffered. Yet, state agencies such as the Department of Financial and Professional Regulation can bring disciplinary actions against licensed health care professionals and impose fines up to \$10,000 along with licensure revocation.

Conversely, the U.S. Department of Health and Human Services (“HHS”) has authority to not only bring administrative actions against covered entities for violations of HIPAA’s Privacy and Security Rules and impose fines up to \$1,500,000, but also coordinate with the Department of Justice for criminal prosecutions of covered entities that bring fines of \$50,000 to \$250,000 and 1-10 years in prison per violation. Furthermore, provisions in the Health Information Technology for Economic and Clinical Health Act (“the HITECH Act”) delegate authority to state attorney generals to bring civil actions against covered entities on behalf of state residents for HIPAA violations. However, the state attorney generals must effectively ask permission from HHS to bring an action against a covered entity and it remains to be seen if Illinois Attorney Generals have initiated such actions.

Texas recently tried to close the gap between state and federal enforcement of PHI privacy and security laws. In September 2012, Texas will increase civil and criminal penalties for PHI privacy violations, create the foundation for inter-agency coordination, implement audits, require breach notification, require certification of covered entities’ privacy and security policies and provide enforcement incentives for government agencies by offering bounties or percentages of recovered damages. Several of the proposals offered in this Briefing Summary follow the principles set forth in Texas’s shift to stronger enforcement since Illinois enforcement of PHI

¹ The General Counsel of OHIT gratefully acknowledges the assistance of John Saran, OHIT Legal Intern, as this paper’s primary author, and the legal research assistance of the following OHIT Legal Interns: Sarah Byers and Pamela Dones.

Re: Privacy Breach Enforcement Briefing Summary

confidentiality likely will need to improve for residents to build trust in the ILHIE's protection of patient data privacy and security.

First, enforcement monitoring procedures could be put in place through the ratification of a breach notification rule that requires covered entities to disclose breaches of PHI and allows resident whistleblowers to report covered entities. Similarly, there should be the technical capability to allow for real-time ILHIE network monitoring and the agency resources for ILHIE Authority field audit teams.

Second, the ILHIE Authority Chief Privacy and Security Officer could manage all enforcement strategies that will include monitoring, coordination with other state agencies, and a budget for enforcement activities and incentives for agency cooperation. Furthermore, the Chief Privacy and Security Officer would review all complaints against covered entities and take the necessary action including referrals to the relevant state agencies enforcing the respective criminal, civil and disciplinary statutory provisions. Finally, OHIT would facilitate the introduction of statutory amendments to follow Texas in raising the criminal penalties for privacy and security violations.

Third, the creation of a breach mitigation strategy would involve requiring covered entities to create a Corrective Action Plan, designate a monitor who reports back to the ILHIE Authority on compliance efforts, provide biannual reports and purchase insurance or provide a monetary fund for those individuals harmed by PHI breaches. Finally, the ILHIE Authority should educate the public on its enforcement efforts through the use of mandatory webinars, a highlights webpage for enforcement activities and educational programs with local non-profit organizations.

II. Illinois Law

The following sections detail and explain all Illinois statutory provisions concerning the enforcement of confidentiality provisions protecting general and other forms of protected health information.

i. General Protected Health Information (PHI)

Statute	Name	Offense/Fine for Breach	Private Right of Action	Enforcement Authority
410 ILCS 50/4	Illinois Medical Patient Rights Act ¹	Petty Offense: \$1,000 Fine	No	Attorney General (AG)/County Attorney (DA)
210 ILCS	Hospital Licensing Act ²	Class A	No	Department

Re: Privacy Breach Enforcement Briefing Summary

85/6.17		Misdemeanor		of Public Health (IDPH)
210 ILCS 45/3-305	Nursing Home Care Act ³	Fines up to \$25,000.	No	IDPH
225 ILCS 60/22	Medical Practice Act of 1987 ⁴	Licensure to \$10,000 fine	No	Department of Financial and Professional Regulation (IDFPR)
215 ILCS 109/5	Dental Care Patient Protection Act ⁵	Fine up to \$1,000	No	Department of Insurance (DI)
225 ILCS 15/15	Clinical Psychologist Licensing Act ⁶	Licensure to \$10,000 fine	No	IDFPR
225 ILCS 20/16	Clinical Social Work and Social Practice Act ⁷	Class A Misdemeanor to Class 4 Felony	No	IDFPR
225 ILCS 55/70	Marriage and Family Therapy Licensing Act ⁸	Class A Misdemeanor to Class 4 Felony	No	IDFPR
225 ILCS 107/75	Professional Counselor and Clinical Professional Counselor Licensing Act ⁹	Licensure to \$10,000 fine; Class A Misdemeanor to Class 4 Felony	No	IDFPR
215 ILCS 134/	Managed Care Reform and Patient Rights Act ¹⁰	Fines up to \$250,000	No	DI
225 ILCS 85	Pharmacy Practice Act ¹¹	Licensure to \$10,000 fine	No	IDFPR

Key: (i) misdemeanor (prison, fine) A²: 12 mos., \$2500; B³: 6 mos., \$1500; C⁴: 30 days, \$1500; (ii) felony (prison, fine) Class 4⁵: 1-3 years, \$25,000/individuals, \$50,000/corporations.

1) The **Illinois Medical Patient Rights Act** protects the patient’s right to privacy and confidentiality when it comes to health care in Illinois.⁶ Physicians, health care providers, health service corporations and insurance companies cannot disclose the ‘nature or details of services’

² 730 ILL. COMP. STAT. 5/5-4.5-55 (2012).

³ 730 ILL. COMP. STAT. 5/5-4.5-60 (2012).

⁴ 730 ILL. COMP. STAT. 5/5-4.5-65 (2012).

⁵ 730 ILL. COMP. STAT. 5/5-4.5-45 (2012).

⁶ 410 ILL. COMP. STAT. 50/3(d) (2012).

Re: Privacy Breach Enforcement Briefing Summary

provided to patients with a few exceptions.⁷ Any physician, health care provider, health services corporation or insurance company that violates the patient's right to privacy and confidentiality through the disclosure of protected information is deemed to have committed a petty offense and subject to a \$1,000 fine.⁸

2) The **Hospital Licensing Act** protects the confidential access to medical records and information contained at Illinois hospitals, licensed through the Illinois Department of Public Health (IDPH).⁹ All medical information gathered at a particular hospital is considered to be property owned by the hospital that must be protected from inappropriate disclosure.¹⁰ No hospital staff member regardless of position may disclose the nature or details of services provided to patients except to the patient, authorized persons and those directly involved in providing care to the patient.¹¹ Any individual who "willfully or wantonly discloses" hospital or medical information is guilty of a Class A misdemeanor.¹² "Willfully and Wantonly" includes a deliberate intention to cause harm to the patient or a conscious indifference or disregard for the safety of patient's information.¹³

3) The **Nursing Home Care Act** protects the privacy and confidentiality of a nursing home resident's medical and personal care program including case discussions, consultations, examination and treatment.¹⁴ The IDPH administers the statute and may impose fines up to \$25,000 depending on the severity of the nursing home's violations that are not corrected.¹⁵

4) The **Medical Practice Act of 1987** governs the licensure of physician and the practice of medicine in Illinois.¹⁶ The Illinois Department of Financial and Professional Regulation (IDFPR) may initiate disciplinary proceedings against a physician for "willfully or negligently violating confidentiality between physician and patient except as required by law."¹⁷ Penalties resulting from a hearing proceeding include revocation or suspension of licenses to the imposition of fines up to \$10,000.¹⁸

5) The **Dental Care Patient Protection Act** protects a dental patient's right to privacy and confidentiality regarding medical and health information.¹⁹ The Director of the Department of

⁷ 410 ILL. COMP. STAT. 50/3(d) (2012).

⁸ 410 ILL. COMP. STAT. 50/4 (2012).

⁹ 210 ILL. COMP. STAT. 85/6.17(d) (2012).

¹⁰ 210 ILL. COMP. STAT. 85/6.17(b) (2012).

¹¹ 210 ILL. COMP. STAT. 85/6.17(d) (2012).

¹² 210 ILL. COMP. STAT. 86/6.17 (i) (2012).

¹³ *Id.*

¹⁴ 210 ILL. COMP. STAT. 45/2-105 (2012).

¹⁵ 210 ILL. COMP. STAT. 45/3-305 (2012).

¹⁶ 225 ILL. COMP. STAT. 60 (2012).

¹⁷ 225 ILL. COMP. STAT. 60/22(a)(30) (2012).

¹⁸ 225 ILL. COMP. STAT. 60/22(a) (2012).

¹⁹ 215 ILL. COMP. STAT. 109/5(b)(4) (2012).

Re: Privacy Breach Enforcement Briefing Summary

Insurance has the power to send managed care dental plans cease and desist orders to compel compliance and the initiation of a correction plan.²⁰ The Director has the discretion to levy a fine up to \$1,000 for unsatisfactory correction, incomplete plans and multiple violations of the Act.²¹

6) The **Clinical Psychologist Licensing Act** protects a patient's right to keep all information given during consultations private and confidential with limited exceptions.²² The IDFPR enforces the statute and may bring disciplinary proceedings against clinical psychologists who violate provisions of the Act²³ or who act in an unauthorized and unprofessional manner.²⁴ Penalties from proceedings could include license suspension or revocation, as well as fines up to \$10,000.²⁵

7) The **Clinical Social Work and Social Practice Act** protects personal information acquired during consulting with social workers in a professional capacity.²⁶ The IDFPR enforces the statute and may bring disciplinary proceedings against social workers who violate specific provisions of the Act.²⁷ Similarly, if not otherwise specified, all violations of the Act including the wrongful disclosure of information are considered a Class A misdemeanor.²⁸ If there is a second conviction or subsequent offense, the violator becomes guilty of a Class 4 felony.²⁹

8) The **Marriage and Family Therapy Act** protects personal information acquired during consulting with marriage and family therapists in a professional capacity.³⁰ The IDFPR enforces the statute and may bring disciplinary proceedings against therapists who violate specific provisions of the Act.³¹ Similarly, if not otherwise specified, all violations of the Act including the wrongful disclosure of information are considered a Class A misdemeanor.³² A subsequent or second offense is a Class 4 felony.³³

9) The **Professional Counselor and Clinical Professional Counselor Licensing Act** provides that all patient information acquired from consultations with the counselor in a professional capacity is privileged.³⁴ The IDFPR has the authority to set fines on violators who commit

²⁰ 215 ILL. COMP. STAT. 109/65 (2012).

²¹ *Id.*

²² 225 ILL. COMP. STAT. 15/5 (2012).

²³ 225 ILL. COMP. STAT. 15/15(5) (2012).

²⁴ 225 ILL. COMP. STAT. 15/15(7) (2012).

²⁵ 225 ILL. COMP. STAT. 15/15 (2012).

²⁶ 225 ILL. COMP. STAT. 20/16 (2012).

²⁷ 225 ILL. COMP. STAT. 20/19 (2012).

²⁸ 225 ILL. COMP. STAT. 20/35 (2012).

²⁹ *Id.*

³⁰ 225 ILL. COMP. STAT. 55/70 (2012).

³¹ 225 ILL. COMP. STAT. 55/85 (2012).

³² 225 ILL. COMP. STAT. 55/160 (2012).

³³ *Id.*

³⁴ 225 ILL. COMP. STAT. 107/75 (2012).

Re: Privacy Breach Enforcement Briefing Summary

specific actions such as malpractice up to \$10,000.³⁵ Similarly, all violations of the Act are considered Class A Misdemeanors on the first offense.³⁶

10) The **Managed Care Reform and Patient Rights Act** provides that a patient has a right to privacy and confidentiality in health care when dealing with health care plans.³⁷ The Director of Insurance may issue cease and desist orders along with a request for correction plan that must be addressed by the health plan.³⁸ A failure to respond to the Director's request or repeated violations of the Act lead to fines up to \$250,000.

11) The **Pharmacy Practice Act** ensures that automated pharmacy systems have privacy and security procedures to protect patient confidentiality and comply with federal law.³⁹ The IDPFR may bring discipline against any pharmacist who discloses PHI in violation of any State or federal law.⁴⁰ Such violation might cause the IDPFR to suspend or revoke the pharmacist's license, or levy fines up to \$10,000.⁴¹

ii. Behavioral Health

Statute	Name	Offense/Fine for Breach	Private Right of Action	Enforcement Authority
740 ILCS 110	Mental Health and Developmental Disabilities Confidentiality Act ¹	Class A Misdemeanor	Yes	AG/DA

Key: (i) misdemeanor (prison, fine) A: 12 mos., \$2500; B: 6 mos., \$1500; C: 30 days, \$1500 (ii) felony (prison, fine) Class 4: 1-3 years, \$25,000/individuals, \$50,000/corporations.

1) The **Mental Health and Developmental Disabilities Confidentiality Act** is the primary behavioral health statute that protects all records and communication from disclosure to those unauthorized persons not exempted in the statute.⁴² Any person who 'knowingly and willfully' performs an action contrary or in violation of the statute is guilty of a Class A misdemeanor.⁴³ Furthermore, any person who is a victim to violations of the Act such as disclosures of information to unauthorized persons may sue for damages, injunctions and litigation/attorney fees.⁴⁴

³⁵ 225 ILL. COMP. STAT. 107/80(a)(6) (2012).

³⁶ 225 ILL. COMP. STAT. 107/160 (2012).

³⁷ 215 ILL. COMP. STAT. 134/5(a)(4) (2012).

³⁸ 215 ILL. COMP. STAT. 134/105 (2012).

³⁹ 225 ILL. COMP. STAT. 85/22(b)(a) (2012).

⁴⁰ 225 ILL. COMP. STAT. 85/30(a)(26) (2012).

⁴¹ 225 ILL. COMP. STAT. 85/30(a) (2012).

⁴² 740 ILL. COMP. STAT. 110/3(a) (2012).

⁴³ 740 ILL. COMP. STAT. 110/16 (2012).

⁴⁴ 740 ILL. COMP. STAT. 110/15 (2012).

Re: Privacy Breach Enforcement Briefing Summary

iii. Alcoholism and Other Drug Abuse Treatment Records

Statute	Name	Offense/Fine for Breach	Private Right of Action	Enforcement Authority
20 ILCS 301	Alcoholism and Other Drug Abuse and Dependency Act¹	Class A Misdemeanor	No	AG/ DA

Key: (i) misdemeanor (prison, fine) A: 12 mos., \$2500; B: 6 mos., \$1500; C: 30 days, \$1500 (ii) felony (prison, fine) Class 4: 1-3 years, \$25,000/individuals, \$50,000/corporations.

1) The **Alcoholism and Other Drug Abuse and Dependency Act** protects all records maintained on a patient involved in programs and activities relating to alcohol and other drug abuse intervention, education, treatment or rehabilitation.⁴⁵ Any person who discloses these records to those not authorized to receive them under the statute is guilty of a Class A Misdemeanor.⁴⁶

iv. HIV/AIDS

Statute	Name	Offense/Fine for Breach	Private Right of Action	Enforcement Authority
410 ILCS 305	AIDS Confidentiality Act¹	Class A Misdemeanor	Yes	AG/ DA

Key: (i) misdemeanor (prison, fine) A: 12 mos., \$2500; B: 6 mos., \$1500; C: 30 days, \$1500 (ii) felony (prison, fine) Class 4: 1-3 years, \$25,000/individuals, \$50,000/corporations.

1) The **AIDS Confidentiality Act** protects the identity and results of patients who seek HIV testing from unauthorized disclosures.⁴⁷ Any person who intentionally or recklessly violates the Act or any regulation promulgated from it is guilty of a Class A Misdemeanor.⁴⁸ Any patient who is aggrieved by a violation of the Act or promulgated regulation has a civil cause of action and can recover for each violation.⁴⁹ For negligent actions, the plaintiff may recover \$2,000 in liquidated damages or actual damages per violation, whichever is greater.⁵⁰ For intentional and reckless actions, the plaintiff may recover \$10,000 in liquidated damages or actual damages per violation, whichever is greater.⁵¹ Finally, the plaintiff may also recover attorney fees⁵² and seek

⁴⁵ 20 ILL. COMP. STAT. 301/30-5(bb) (2012).

⁴⁶ 20 ILL. COMP. STAT. 301/30-5(bb)(5) (2012).

⁴⁷ 410 ILL. COMP. STAT. 305/9 (2012).

⁴⁸ 410 ILL. COMP. STAT. 305/12 (2012).

⁴⁹ 410 ILL. COMP. STAT. 305/13 (2012).

⁵⁰ 410 ILL. COMP. STAT. 305/13(1) (2012).

⁵¹ 410 ILL. COMP. STAT. 305/13(2) (2012).

⁵² 410 ILL. COMP. STAT. 305/13(3) (2012).

Re: Privacy Breach Enforcement Briefing Summary

any other necessary relief including injunctions.⁵³ The confidentiality protection and enforcement provisions of the **AIDS Confidentiality Act** also apply to reports of cases of perinatal HIV to the Department of Public Health by health care facilities pursuant to the **Perinatal HIV Prevention Act**.⁵⁴

v. Sexually Transmitted Diseases

Statute	Name	Offense/Fine for Breach	Private Right of Action	Enforcement Authority
410 ILCS 325	Illinois Sexually Transmitted Disease Control Act ¹	\$500 per violation	No	IDPH

Key: (i) misdemeanor (prison, fine) A: 12 mos., \$2500; B: 6 mos., \$1500; C: 30 days, \$1500 (ii) felony (prison, fine) Class 4: 1-3 years, \$25,000/individuals, \$50,000/corporations.

1) The **Illinois Sexually Transmitted Disease Control Act** requires physicians and other health care professionals to report positive test results of sexually transmitted diseases to the Department of Public Health.⁵⁵ All persons required to report under the Act must maintain strict confidentiality of all information/records.⁵⁶ Upon notice and a hearing, the Department of Public Health may institute a \$500 fine to any person, laboratory or blood bank violating the privacy and confidentiality provisions of the Act.⁵⁷ The Department of Public Health then must report the violation to the regulatory agency that grants the person or entity a license to do business in Illinois.⁵⁸

vi. Public Health Reporting

Statute	Name	Offense/Fine for Breach	Private Right of Action	Enforcement Authority
410 ILCS 525	Illinois Health and Hazard Substances Registry Act ¹	Class A Misdemeanor; \$1,000 fine per violation	No	AG/ DA

Key: (i) misdemeanor (prison, fine) A: 12 mos., \$2500; B: 6 mos., \$1500; C: 30 days, \$1500 (ii) felony (prison, fine) Class 4: 1-3 years, \$25,000/individuals, \$50,000/corporations.

⁵³ 410 ILL. COMP. STAT. 305/13(4) (2012).

⁵⁴ 410 ILL. COMP. STAT. 15/(c) (2012).

⁵⁵ 410 ILL. COMP. STAT. 325/4 (2012).

⁵⁶ ILL. ADMIN CODE tit. 77, § 693.30 (2012).

⁵⁷ ILL. ADMIN CODE tit. 77, § 693.35(a) (2012).

⁵⁸ ILL. ADMIN CODE tit. 77, § 693.35(b) (2012).

Re: Privacy Breach Enforcement Briefing Summary

1) The **Illinois Health and Hazard Substances Registry Act** requires hospitals and laboratories to report the incidence of cancer conditions and treatment to a state registry.⁵⁹ The Act specifically provides that the identity or collective medical facts of a patient are to be confidential.⁶⁰ Any person who violates the Act is guilty of a Class A Misdemeanor⁶¹ and may be liable for a civil penalty not to exceed \$1,000 per violation.⁶²

vii. Abuse Reporting

Statute	Name	Offense/Fine for Breach	Private Right of Action	Enforcement Authority
325 ILCS 5	Abused and Neglected Child Reporting Act ¹	Class A Misdemeanor	No	AG/DA
325 ILCS 15	Child Sexual Abuse Prevention Act ²	Class A Misdemeanor	No	AG/DA

Key: (i) misdemeanor (prison, fine) A: 12 mos., \$2500; B: 6 mos., \$1500; C: 30 days, \$1500 (ii) felony (prison, fine) Class 4: 1-3 years, \$25,000/individuals, \$50,000/corporations.

1) The **Abused and Neglected Child Reporting Act** requires the Department of Child and Family Services to act upon reports of child abuse.⁶³ Any information gathered by the Department is confidential and anyone who permits, assists or encourages the unauthorized disclosure of this information is guilty of a Class A Misdemeanor.⁶⁴

2) The **Child Sexual Abuse Prevention Act** permits the Department of Children and Family Services to develop programs and services to prevent child sexual abuse. The confidential and enforcement provision are the same as the **Abused and Neglected Child Reporting Act**.

viii. Medical Research

Statute	Name	Offense/Fine for Breach	Private Right of Action	Enforcement Authority
410 ILCS 520	Illinois Health Statistics Act ¹	Class C Misdemeanor	No	AG/DA
735 ILCS 5/8-2101	Illinois Code of Civil Procedure - Medical Studies ²	Class A Misdemeanor	No	AG/DA

⁵⁹ 410 ILL. COMP. STAT. 525/4(b) (2012).

⁶⁰ 410 ILL. COMP. STAT. 525/4(d) (2012).

⁶¹ 410 ILL. COMP. STAT. 525/13(a) (2012).

⁶² 410 ILL. COMP. STAT. 525/13(b) (2012).

⁶³ 325 ILL. COMP. STAT. 5/2 (2012).

⁶⁴ 325 ILL. COMP. STAT. 5/11 (2012).

Re: Privacy Breach Enforcement Briefing Summary

Key: (i) misdemeanor (prison, fine) A: 12 mos., \$2500; B: 6 mos., \$1500; C: 30 days, \$1500 (ii) felony (prison, fine) Class 4: 1-3 years, \$25,000/individuals, \$50,000/corporations.

1) The **Illinois Health Statistics Act** allows the Department of Public Health to collect, research and analyze health statistics on illnesses, obesity and disabilities.⁶⁵ Any person who intentionally, wantonly or willfully discloses identifiable health data collected under this Act is guilty of a Class C Misdemeanor.

2) The **Illinois Code of Civil Procedure** protects the confidentiality of all patient records used in medical studies.⁶⁶ Anyone convicted of unlawful or unauthorized disclosure is guilty of a Class A Misdemeanor.⁶⁷

ix. Genetic Testing

Statute	Name	Offense/Fine for Breach	Private Right of Action	Enforcement Authority
410 ILCS 513	Genetic Privacy Information Act ¹	Civil Suit Damages: \$2,500 - \$15,000+	Yes	None
225 ILCS 135	Genetic Counselor Licensing Act ²	Licensure, Fine up to \$1,000	No	IDFPR

Key: (i) misdemeanor (prison, fine) A: 12 mos., \$2500; B: 6 mos., \$1500; C: 30 days, \$1500 (ii) felony (prison, fine) Class 4: 1-3 years, \$25,000/individuals, \$50,000/corporations.

1) The **Genetic Privacy Information Act** protects the confidentiality of genetic testing information.⁶⁸ A person aggrieved by violations of this Act may seek civil relief where the person can recover damages, reasonable attorneys' fees and any other such relief.⁶⁹ A negligent violation brings damages of at least \$2,500 per violation or the amount of actual damages, whichever is greater.⁷⁰ An intentional or reckless violation brings damages of at least \$15,000 per violation or the amount of actual damages, whichever is greater.⁷¹

⁶⁵ 410 ILL. COMP. STAT. 4(a) (2012).

⁶⁶ 735 ILL. COMP. STAT. 5/8-2101 (2012).

⁶⁷ 735 ILL. COMP. STAT. 5/8-2105 (2012).

⁶⁸ 410 ILL. COMP. STAT. 513/15 (2012).

⁶⁹ 410 ILL. COMP. STAT. 513/40(a) (2012).

⁷⁰ 410 ILL. COMP. STAT. 513/40(a)(1) (2012).

⁷¹ 410 ILL. COMP. STAT. 513/40(a)(2) (2012).

Re: Privacy Breach Enforcement Briefing Summary

2) The **Genetic Counselor Licensing Act** provides for the regulation and licensing of genetic counselors in Illinois.⁷² The Act protects the confidentiality of information acquired by the genetic counselors from patients.⁷³ The IDPR may bring disciplinary actions against genetic counselors for failing to maintain the confidentiality of information received from the client.⁷⁴ The Department may suspend or revoke the genetic counselor's license, or initiate fines up to \$1,000 per violation.⁷⁵

j) Identity Theft

Statute	Name	Offense/Fine for Breach	Private Right of Action	Enforcement Authority
720 ILCS 5	Criminal Code of 1961: Identity Theft¹	Class 4+ felony	Yes	AG

Key: (i) misdemeanor (prison, fine) A: 12 mos., \$2500; B: 6 mos., \$1500; C: 30 days, \$1500 (ii) felony (prison, fine) Class 4: 1-3 years, \$25,000/individuals, \$50,000/corporations.

1) **The Criminal Code of 1961** provides that a person can commit the crime of identity theft by using personal information to obtain services,⁷⁶ selling or transferring personal information knowing that the information was stolen or produced without authorization⁷⁷ or using personal information to portray him or herself as the person.⁷⁸ A person convicted of identity theft when using personal information to obtain credit, property or services and the property is worth less than \$300, is guilty of a minimum offense of a Class 4 felony.⁷⁹ For property worth between \$300 and \$2,500, the minimum offense is a Class 3 felony.⁸⁰ The next range is property worth \$2,500 to \$10,000 that carries a minimum of a Class 2 felony.⁸¹ Furthermore, for property worth between \$10,000 and \$100,000, the minimum is a Class 1 felony.⁸² Finally, the theft of property over \$100,000 carries a minimum of a Class X felony.⁸³ For those convicted of identity theft for any other reason, the sentence carries a sentence of a Class 3 felony.⁸⁴ That sentence increases with repeated or subsequent offenses.⁸⁵

⁷² 225 ILL. COMP. STAT. 135/5 (2012).

⁷³ 225 ILL. COMP. STAT. 135/90(a) (2012).

⁷⁴ 225 ILL. COMP. STAT. 135/95(a)(10) (2012).

⁷⁵ 225 ILL. COMP. STAT. 135/95(a) (2012).

⁷⁶ 720 ILL. COMP. STAT. 5/16-30(a)(1) (2012).

⁷⁷ 720 ILL. COMP. STAT. 5/16-30(a)(4) (2012).

⁷⁸ 720 ILL. COMP. STAT. 5/16-30(a)(6) (2012).

⁷⁹ 720 ILL. COMP. STAT. 5/16-30(e)(1)(A)(i) (2012).

⁸⁰ 720 ILL. COMP. STAT. 5/16-30(e)(1)(A)(i)(ii) (2012).

⁸¹ 720 ILL. COMP. STAT. 5/16-30(e)(1)(A)(i)(iii) (2012).

⁸² 720 ILL. COMP. STAT. 5/16-30(e)(1)(A)(i)(iv) (2012).

⁸³ 720 ILL. COMP. STAT. 5/16-30(e)(1)(A)(i)(v) (2012).

⁸⁴ 720 ILL. COMP. STAT. 5/16-30(e)(1)(B) (2012).

⁸⁵ 720 ILL. COMP. STAT. 5/16-30(e)(1)(C-D) (2012).

III. Federal Law

The Department of Health Human Services, Office of Civil Rights (OCR) enforces HIPAA's Privacy and Security Rules.⁸⁶ OCR will either review complaints submitted by patients or other persons against covered entities or conduct its own compliance review of covered entities.⁸⁷ If OCR suspects a criminal violation of HIPAA, then it will refer the complaint to the Department of Justice.⁸⁸ All civil violations lead to agency investigation and adjudication where the covered entity could be subject to civil penalties upon an administrative hearing.⁸⁹ Furthermore, state attorney generals have the authority to bring actions on behalf of state residents against covered entities to recover damages for HIPAA's Privacy and Security Rule violations.⁹⁰

Between September 2009 and April 30, 2012, OCR received 421 reports involving a breach of protected health information affecting over 500 individuals pursuant to the HITECH Breach Notification Rule.⁹¹ Of those reports, 65% involved the theft or loss of PHI.⁹² However, for breaches of protected health information that involve under 500 individuals, there were 57,000+ reports during that period.⁹³ The risks of storing and transporting electronic PHI is tremendous with single stolen back-up tapes affecting 5 million people or the theft of a desktop computer affecting nearly 1 million.⁹⁴

With Illinois having the 5th largest population in the United States, it is likely that thousands of breaches occur in Illinois. While it is presently unknown to what extent creation and operation of the ILHIE would increase risk of unauthorized disclosure, single users will be able to access PHI of hundreds of thousands if not millions of state residents. Thus, it is still worth reviewing the harsh federal civil and criminal penalties under HIPAA to use as a guide for improving Illinois law to foster trust in the ILHIE's protection of patient data.

⁸⁶ *How OCR Enforces the HIPAA Privacy Rule*, U.S.D.H.H.S., <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html>, (last visited July 8, 2012).

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *Id.*

⁹⁰ Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §17939 (2012).

⁹¹ 45 C.F.R. 164.408.

⁹² Marilou King, U.S.D.H.H.S., O.C.R., O.G.C., Presentation at the American Health Lawyers Association Annual Meeting: HITECH Breach Notification Requirements and Reporting Trends, (June 25-27, 2012).

⁹³ *Id.*

⁹⁴ *Id.*

Re: Privacy Breach Enforcement Briefing Summary

Civil Penalties

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

On October 30, 2009, the Secretary of HHS issued an interim final rule that amended HIPAA’s civil penalty enforcement provisions to parallel those set forth in the HITECH Act.⁹⁵ These provisions comprise of tiered ranges of civil monetary penalties for violations of HIPAA, which would include unauthorized disclosure of protected health information.⁹⁶ The interim rule became effective on November 30, 2009 and HHS never promulgated a final rule making the interim rule binding federal guidance.⁹⁷

The minimum violation occurs when a covered entity did not have knowledge of the violation and would not have discovered the violation with reasonable diligence.⁹⁸ Reasonable diligence means the “business care and prudence expected from a person seeking a legal requirement under similar circumstances.”⁹⁹ The penalty range per violation for this level is \$100 to \$25,000 depending on the circumstances.¹⁰⁰ If there are multiple violations of a single provision within a calendar year, the Secretary cannot impose more than a \$1,500,000 fine.¹⁰¹ The Secretary of HHS determines identical violations of single provision or prohibition based on the type of obligations the provision requires including the number of persons or timeframe required.¹⁰² If a covered entity continuously violates a provision, a separate violation occurs every day the covered entity continues to be in violation of the provision.¹⁰³

The second tier violation occurs when the covered entity’s violation was due to reasonable cause and not willful neglect.¹⁰⁴ ‘Reasonable cause’ means that it was unreasonable for the covered entity given the circumstances and despite the exercise of ordinary business care and

⁹⁵ HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56,123 (Oct. 30, 2009) (to be codified at 45 C.F.R. pt. 160).

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ 45 C.F.R. 160.404 (b)(2)(i).

⁹⁹ 45 C.F.R. 160.401.

¹⁰⁰ 45 C.F.R. 160.404 (b)(2)(i).

¹⁰¹ *Id.*

¹⁰² 45 C.F.R. 160.406.

¹⁰³ *Id.*

¹⁰⁴ 45 C.F.R. 160.404 (b)(2)(ii).

Re: Privacy Breach Enforcement Briefing Summary

prudence to comply with the provision.¹⁰⁵ “Willful neglect” means when a covered entity consciously or intentionally fails to comply with a provision, or is recklessly indifferent to complying with the obligation of the provision.¹⁰⁶ The range of civil penalties for “a reasonable cause” violation is \$1,000 to \$50,000 per violation, with a maximum of \$1,500,000 for multiple violations within a calendar year.¹⁰⁷

The final two violations occur when a covered entity is found to have violated a provision with “willful neglect.”¹⁰⁸ If the covered entity corrected the violation within a 30-day period beginning on the first date that the covered entity knew or reasonably should have known about the violation, then the covered entity is only subject to a penalty range of \$10,000 to \$50,000, with an aggregate of multiple identical violations of \$1,500,000.¹⁰⁹ If the covered entity does not correct the violation within 30 days, then the penalty per violation is at least \$50,000, with an aggregate maximum of \$1,500,000 for identical violations within a calendar year.¹¹⁰

Criminal Penalties

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

HIPAA provides a tiered range of criminal penalties for offenses where a person knowingly misuses PHI, obtains PHI of another person or discloses PHI to another person in violation of the statute.¹¹¹ A person violates the Act when he obtains PHI maintained by a covered entity and discloses the information without authorization.¹¹² The minimum penalty is a fine up to \$50,000 and/or up to one year imprisonment.¹¹³ If a person commits an offense under false pretenses or fraud, the fine moves up to \$100,000 and imprisonment up to five years.¹¹⁴ Finally, if a person commits the offense “with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm,” he will be fined up to \$250,000 and/or up to ten years in prison.¹¹⁵

¹⁰⁵ 45 C.F.R. 160.401.

¹⁰⁶ *Id.*

¹⁰⁷ 45 C.F.R. 160.404 (b)(2)(ii).

¹⁰⁸ 45 C.F.R. 160.404 (b)(2)(iii).

¹⁰⁹ *Id.*

¹¹⁰ 45 C.F.R. 160.404 (b)(2)(iv).

¹¹¹ Social Security Act, 42 U.S.C. §1320d-6(a) (2012).

¹¹² *Id.*

¹¹³ Social Security Act, 42 U.S.C. §1320d-6(b) (2012).

¹¹⁴ *Id.*

¹¹⁵ *Id.*

Re: Privacy Breach Enforcement Briefing Summary

State Attorney General Authority

The HITECH Act amended the Social Security Act to grant all State Attorney General (SAG) authority to bring civil actions against covered entities for HIPAA Privacy and Security Rule violations on behalf of state residents.¹¹⁶ These civil actions allow for SAG's to collect damages, enjoin further violations¹¹⁷ and possibly retain attorney fees.¹¹⁸ Each violation can win up to \$100 in damages with the aggregate total of violations bringing no more than \$25,000.¹¹⁹ However, SAGs interested in filing civil complaints must serve HHS prior to bringing an action against a covered entity.¹²⁰ Also, OCR created HIPAA Enforcement Training to help State Attorney Generals and their staff enforce HIPAA's Privacy and Security Rules.¹²¹

IV. Other State's Best Practice: Texas

One example of a state strengthening closing the state and federal enforcement gap regarding PHI privacy and security occurs in Texas.¹²² Effective September 1, 2012, H.B. 300 will amend the Texas Health and Safety Code and Business and Commerce Code in a manner that increases the State Attorney General's enforcement powers and all fines and penalties.¹²³ The following points are all key bill provisions that inspire several of this Briefing Summary's proposals.

Key Bill Provisions:

1. Attorney General will maintain a **consumer information website** that will detail (1) consumer privacy rights; (2) list of state agencies that regulate covered entities; (3) each agency's compliance enforcement powers and procedures and (4) contact information for each agency that you can report violations of the Health and Safety Code including prohibited uses of protected health information.¹²⁴
2. **Civil penalties** from actions brought by the Attorney General against covered entities will be increased.¹²⁵ For negligent actions, the penalty will rise from \$3,000 to \$5,000 per violation.¹²⁶ For violations committed with knowledge or intention, the penalty

¹¹⁶ Social Security Act, 42 U.S.C. §1320d-5(d) (2012).

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ *Id.*

¹²¹ *HIPAA Enforcement Training for State Attorneys General*, U.S.D.H.H.S., <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/sagmoreinfo.html>, (last visited July 10, 2012).

¹²² 2011 TEX. H.B. 300.

¹²³ *Id.*

¹²⁴ TEX. HEALTH & SAFETY CODE § 181.103.

¹²⁵ § 181.201(b).

¹²⁶ § 181.201(b)(1).

Re: Privacy Breach Enforcement Briefing Summary

- will be \$25,000 per violation.¹²⁷ For violations committed with the intent to sell PHI for financial gain, the penalty is \$250,000 per violation.¹²⁸
3. **Cooperation from licensing agencies** responsible for regulating covered entities and the Attorney General in that the licensing agency must refer the matter to the Attorney General.¹²⁹
 4. **Bounties** from these civil actions are allowed where the Attorney General may retain a reasonable portion of a civil penalty¹³⁰ not to exceed an amount to be determined by the Texas Legislature.
 5. A **catch-all disciplinary provision** that gives licensing agencies an enumerated statutory provision for bringing disciplinary actions against licensed covered entities for violations of the Act.¹³¹ The agency can either revoke a license for egregious violations or patterns of conduct, or refer the violations to the Attorney General for civil action.¹³²
 6. **Penalty determination** for covered entities by courts need to consider various factors including:¹³³
 - a. Seriousness of the violation and disclosure;
 - b. Compliance history;
 - c. Potential risk of causing financial, reputational or other harm to the affected individual;
 - d. Deterrence for future violations; and
 - e. Efforts to correct the violation.
 7. The Attorney General and various other state agencies may request that HHS conduct **audits** of covered entities in Texas.¹³⁴ These agencies will monitor these audits, request copies of all compliance work done by the covered entities and submit reports to the Texas Legislature.¹³⁵

¹²⁷ § 181.201(b)(2).

¹²⁸ § 181.201(b)(3).

¹²⁹ § 181.201(e).

¹³⁰ § 181.201(f).

¹³¹ § 181.202.

¹³² § 181.202(1-2).

¹³³ TEX. HEALTH & SAFETY CODE § 181.205(b)

¹³⁴ § 181.206.

¹³⁵ TEX. HEALTH & SAFETY CODE § 181.206.

Re: Privacy Breach Enforcement Briefing Summary

8. **Certification** requirement where a covered entity needs to develop and submit its privacy and security standards surrounding the electronic sharing of PHI to the Health and Human Services Commission.¹³⁶
9. **Required notification** by anyone conducting business in the state of breaches of sensitive personal information to any individual, regardless of state residency.¹³⁷ A failure to report such breaches is a \$100 per day violation that cannot exceed \$250,000 in a calendar year.¹³⁸
10. **Criminal penalty increase** for identity theft via an electronic device from a Class B Misdemeanor to a state jail felony for someone who accesses, reads, stores or transfers PHI encrypted on a payment card with the intent to harm or defraud another.¹³⁹

V. Proposals to Foster Public Trust in the ILHIE

i. Enforcement Monitoring

- i) Establish breach reporting rule so that HIE can quickly mitigate any damage and take enforcement action or make referrals to other state agencies, e.g. state attorney's office or IDFPR.
 - (1) By breached entities upon discovery.
 - (2) By public whistleblowers with some financial incentive.
- ii) Establish the technical infrastructure within the HIE to allow for real-time network monitoring for privacy and security breaches.
- iii) Establish ILHIE field audit teams.
 - (1) HIE/HHS audits of participants.
 - (2) Private third-party audits of participants.
 - (3) User self-certification of audit.

ii. Enforcement Strategies

- i) Appointment of an ILHIE Authority Chief Privacy and Security Officer (CPSO)
 - (1) Oversee and manage all enforcement monitoring and audits
 - (2) Manage budget for enforcement activities and incentives for inter-agency cooperation
 - (3) Coordinate with other agencies for enforcement
 - (4) Review all complaints actions against covered entities

¹³⁶ § 181.108.

¹³⁷ TEX BUS. & COM. CODE § 521.053(b).

¹³⁸ § 521.151 (a-1).

¹³⁹ § 522.002(b).

Re: Privacy Breach Enforcement Briefing Summary

- (5) Manage mitigation of breaches
- (6) Direct public education
- ii) ILHIE coordinates state government enforcement of privacy breaches with the Attorney General, Office of Inspector General, Health and Family Services and County State Attorneys.
- iii) ILHIE proposes the following increased IL criminal penalties for privacy breaches and non-compliance with HIPAA's Privacy and Security Rules. The CPSO would have discretion to either refer complaints to the Illinois Attorney General for criminal prosecution or the relevant state agencies for civil and administrative actions.
 - (1) Class A Misdemeanor minimum with fines up to \$25,000 per violation;
 - (2) Class 4 felony for negligence with fines from \$25,000-\$50,000; (<1 yr)
 - (3) Class 3 felony for gross negligence/reckless disregard with fines from \$50,000-\$75,000; (<2 yrs)
 - (4) Class 2 felony for false pretenses with fines from \$75,000-\$100,000; (3-5 yrs)
 - (5) Class 1 felony for intent to sell/cause malicious harm with fines from \$100,000-\$250,000; (4-10 yrs).

iii. Breach Mitigation Strategies

- i) The CPSO will demand a Corrective Action Plan from the covered entity that 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
- ii) The CPSO will designate a monitor (normally the covered entity's Chief Privacy Officer) who will report back to the ILHIE on the ongoing compliance efforts.
- iii) The CPSO will collect biannual reports on the implementation of compliant processes and procedures for one year.
- iv) The CPSO will facilitate the covered entity purchasing insurance or setting aside funds for the mitigation of injuries to patients.

iv. Education of the Public

- i) Maintain a webpage linked to the ILHIE website focused on enforcement reporting similar to HHS's <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html>.
- ii) Quarterly webinars discussing enforcement activity and breach notifications, where participants must attend one per year.
- iii) Solicit non-profit organizations for public education programs in exchange for grant money regarding topics of privacy and security management, breach reporting and public trust.

July 17, 2012