Illinois Public Health Association

Impact of HIPAA on Public Health...Now.
Shefali Mookencherry, MPH, MSMIS, RHIA, CHPS, HCISPP
Presenter
January 22, 2016
Session 2 of 2

Presenter Introduction
Shefali Mookencherry, MPH, MSMIS, RHIA, CHPS, HCISPP
Shefali Mookencherry has extensive experience in the HIPAA, healthcare IT/finance, Meaningful Use, and revenue cycle areas, including 20+ years in the healthcare industry, with nine spent in senior management positions.

She has conducted HIPAA education, training, compliance assessments/analyses for various clients including small physician practices, IT vendors to larger integrated delivery networks and academic institutions.

Shefali is certified in national and international privacy and security regulations. Furthermore, She teaches graduate students at a local University about HIPAA, health insurance exchanges, revenue cycle, healthcare reform, and IT security.

Assumptions
- Certain information in this presentation comes from a variety of sources such as:
  - CMS (their website cms.gov)
  - Illinois General Assembly (Public Acts/legislation)
  - Illinois Department of Healthcare and Family Services (HFS)
  - Industry blogs, journals, etc.
  - Office of Civil Rights (hhs.gov/ocr)

Disclaimer: The materials for this presentation are for informational purposes only. Information on this topic does not constitute legal or business advice. Information in this presentation is provided without warranty of any kind, either expressed or implied, including but not limited to, the implied warranties of fitness for a particular purpose.

Objectives
- Review HIPAA compliance within various scenarios
- Public Health activities vs. other Federal regulations (i.e.: HIV reporting, etc.)
- Know how to protect PHI/ePHI with compliance activities
  - HIPAA compliance assessments
  - HIPAA IT Security Risk Analysis
  - HIPAA education
  - HIPAA enforcement
- Understand your role in protecting privacy and the consequences for violations

Illinois Freedom of Information (FOI) Laws
- FOI laws exempt from disclosure “information not subject to disclosure under another law.”
- Public is prohibited access to:
  - Either public records or identifiable information in public records declared confidential by state statute
  - Communicable disease reports
  - HIV patient data
  - Patient medical records
  - Immunization data
  - Cancer registries
  - Vital records

Public Health Activities vs. Other Federal Regulations
Illinois Freedom of Information Laws

- Access is prohibited when federal privacy laws prohibit disclosure:
  - Educational records protected by the FERPA
  - Substance abuse diagnosis and treatment records covered by federal regulations
  - Identifiable information about veterans or their families covered by the VA Claims Confidentiality Statute

(20 ILCS 2305/) IL Department of Public Health Act

- All access to data by the Department, reports made to the Department, the identity of or facts that would tend to lead to the identity of the individual who is the subject of the report, and the identity of or facts that would tend to lead to the identity of the author of the report shall be strictly confidential, are not subject to inspection or dissemination, and shall be used only for public health purposes by the Department, local public health authorities, or the Centers for Disease Control and Prevention.

Public Health Protect Health Information (PHI)

- Immunizations registries/results
- Mental Health records
- Drug and Alcohol Abuse records
- AIDS/HIV test results
- Controlled substance medication history from IL prescription monitoring program (PMP)
- Newborn screenings (metabolic and hearing)
- Lead results
- STD results registries
- Test results from state labs
- Communicable disease test results registries (Tuberculosis)
- Cancer registries
- Other PHI held

Immunization Information

Uses and Disclosures

What: Student Immunizations

- CEs are permitted to disclose proof of immunization to a school where state or other law requires the school to have such information prior to admitting the student.
- Written authorization is no longer required for this disclosure, but CEs will still be required to obtain agreement, which may be oral, from a parent, guardian or other person acting in loco parentis, or from the individual himself or herself, if the individual is an adult or emancipated minor.
- The CE must document the agreement obtained.

Immunization Disclosure -IL

(410 ILCS 527/20)

Sec. 20. Confidentiality of information; release of information; statistics; panel on expanding access.

(a) Records maintained as part of the immunization data registry are confidential.

(b) The Department may release an individual’s confidential information to the individual or to the individual’s parent or guardian if the individual is less than 18 years of age.
Immunization Disclosure - IL
(410 ILCS 527/20)
Sec. 20. Confidentiality of information; release of information; statistics; panel on expanding access. (Continued)
(c) Subject to subsection (d) of this Section, the Department may release information in the immunization data registry concerning an individual to the following entities:
(1) The immunization data registry of another state.
(2) A health care provider or a health care provider's designee.
(3) A local health department.
(4) An elementary or secondary school that is attended by the individual.
(5) A licensed child care center in which the individual is enrolled.
(6) A licensed child-placing agency.
(7) A college or university that is attended by the individual.
(8) The Department of Healthcare and Family Services or a managed care entity contracted with the Department of Healthcare and Family Services to coordinate the provision of medical care to enrollees of the medical assistance program.

(d) Before immunization data may be released to an entity, the entity must enter into an agreement with the Department that provides that information that identifies a patient will not be released to any other person without the written consent of the patient.
(e) The Department may release summary statistics regarding information in the immunization data registry if the summary statistics do not reveal the identity of an individual. (Source: P.A. 97-117, eff. 7-14-11; 98-651, eff. 6-16-14.)

Immunization Disclosure - IL
(410 ILCS 527/25)
Sec. 25. Immunity for providing data; penalty.
(a) An entity described in subsection (c) of Section 20 of this Act, the Department, or an agent of the Department who in good faith provides or receives immunization information is immune from civil and criminal liability for the following actions:
(1) Providing information to the immunization data registry.
(2) Using the immunization data registry information to verify that a patient or child has received proper immunizations.
(3) Using the immunization data registry information to inform a patient or the child's parent or guardian of the patient's or child's immunization status or that an immunization is due according to recommended immunization schedules.
(b) A person who knowingly, intentionally, or recklessly discloses confidential information contained in the immunization data registry in violation of this Act commits a Class A misdemeanor. (Source: P.A. 97-117, eff. 7-14-11.)

Cancer Registry
Uses and Disclosures
State cancer registry. Under a state law, health-care providers are required to report cancer cases to a state's cancer registry. Names are included to prevent duplicate reporting and counting. State law protects the confidentiality of the data. Can covered entities disclose the information under the Privacy Rule?
Privacy Rule effect. Covered entities may disclose PHI to a public health agency, or any other entity, when the disclosure is required by law. However, the covered entities must be prepared to account for the disclosures if requested by the persons whose PHI has been shared. The state agency may use and further disclose the PHI consistent with applicable state law.

Lead Testing and Reporting
Uses and Disclosures
Lead Testing and Reporting

- Every physician who diagnoses, or health care provider, nurse, hospital administrator, or public health officer who has verified information of any person who has a level of lead in the blood in excess of the permissible limits, as defined in Section 845.20, is required to report pursuant to this Section, starting with a confirmed lead level of 10 mcg/dL. (Section 7 of the Act)

- If the analysis has been performed at the State laboratory, or the provider has ascertained that the clinical laboratory where specimens are processed electronically reports all blood lead level results to the Department, then duplicate reporting of elevated levels is not required.

- Upon the request of a provider, the Department may generate a list of individual patients treated by that provider according to the claims records and the patients’ lead test results. (Section 6.3(b) of the Act)

Mental Health Uses and Disclosures

Illinois’ Mental Health and Developmental Disabilities Confidentiality Act (“MHDDCA”) 740 ILCS 110/1

- Governs all Illinois providers of mental health or developmental disabilities services.

- Offers broad privacy and confidentiality protections for mental health records and treatment information.

MHDDCA, 740 ILCS 110/1

- Absent an exception, MHDDCA prohibits all unauthorized disclosures of mental health records or treatment information by requiring an individual’s consent before a provider may disclose mental health records or communications.

- In the event of a conflict between the application of the Physician-Patient’s Act and the Mental Health and Developmental Disabilities Confidentiality Act, the provisions of the MHDDCA shall control.

Drug and Alcohol Abuse Uses and Disclosures
Federal Drug and Alcohol Confidentiality Regulations

- Two laws enacted in the early 1970's (one for alcohol, one for drugs)
- Guarantee strict confidentiality of information about persons receiving alcohol and drug prevention and treatment services
- Regulations implementing the statues were issued in 1975
- Amended in 1987: Mandated abuse reporting
- Consolidated the statutes in 1992 (42 U.S.C. 290-2), the regulations were not changed (42 CFR Part 2)

Applicability

- Any information (including referral and intake) about alcohol and drug abuse patients obtained by a program
- Includes (not limited to):
  - Treatment or rehab programs
  - EAP
  - Programs within a general hospital
  - School-based programs
  - Private practitioners who provide alcohol or drug abuse diagnosis, treatment or referral

Intent of 42 CFR Part 2

- Insure that an alcohol or drug abuse patient is not made more vulnerable by reason of the availability of his or her patient record than an individual who has an alcohol or drug problem and who does not seek treatment.
- Regulations PROHIBIT the disclosure and use of patient records, with a few exceptions.
- Disclosure MAY occur if an exception exists but it does not REQUIRE the disclosure (except with a court order).

42 CFR Part 2 Allowable Disclosures

- Written authorization
- Internal communication ("need to know")
- No patient-identifying information
- Medical emergency
- Qualified Service Organization
- Audit and evaluation
- Crimes (or threats of) on program premises or against program personnel
- Initial reports of suspected child abuse or neglect
- Court order meeting specifications of 42
- Research

More interesting 42 CFR Part 2 facts

- Applies even if the person seeking the information already has it or has other ways to obtain it
- Applies to law enforcement or other official, even with a subpoena
- Disclosing even the presence of a patient at a facility or unit which is identified as a place where only drug/alcohol services are provided requires written authorization

Which “wins”? 

- Generally, the more recently enacted, HOWEVER:
  - Not if earlier law has a more narrow, precise, or specific subject
  - Not if later law addresses an issue on which an earlier law was silent
Continued…

- Many HIPAA provisions PERMIT something but don’t mandate it.

- 42 CFR Part 2 PROHIBITS all disclosures unless specifically allowed by the regulation.

Examples of Rule Conflicts

Disclosure for Payment

- HIPAA PERMITS disclosure without patient consent for the purpose of payments.

- 42 CFR Part 2 PROHIBITS these disclosures without patient consent.

Providers must follow 42 CFR Part 2.

Patient Rights & Administrative Requirements

- HIPAA imposes several new administrative requirements and establishes new patient rights.

- These are not included in 42 CFR Part 2.

Providers must follow HIPAA.

Personal Representatives

- HIPAA permits a “personal representative” (e.g. power of attorney) to sign consent forms on behalf of the patient.

- 42 CFR Part 2 limits those who may act in the place of the patient to individuals who have been legally appointed the patients’ guardian.

Providers must follow 42 CFR Part 2.

Re-disclosure of Information

- HIPAA is silent on this topic.

- 42 CFR Part 2 requires that a statement prohibiting re-disclosure accompanies the patient information that is disclosed.

Providers must follow 42 CFR Part 2.
Disclosures to Other Providers
- HIPAA allows, but does not require, programs to make disclosures to other healthcare providers without authorization.
- 42 CFR Part 2 limits this to medical emergencies.

Providers must follow 42 CFR Part 2.

Medical Emergencies
- HIPAA allows health care providers to inform family members of the individual's location and condition without consent in emergency circumstances or if a person is incapacitated.
- 42 CFR Part 2 limits this disclosure to medical personnel ONLY.

Providers must follow 42 CFR Part 2.

Disclosure to Public Health
- HIPAA permits disclosure to a public health authority for disease prevention or control, or to a person who may have been exposed to or at risk of spreading a disease or condition.
- 42 CFR Part 2 prohibits these disclosures unless there is an authorization, court order, or the disclosure is done with out revealing patient information.

Providers must follow 42 CFR Part 2.

Court Orders
- HIPAA makes no mention of any standards or procedures that a court must follow when issuing a court order.
- 42 CFR Part 2 has specific requirements.

Providers must follow 42 CFR Part 2.

Disclosure of Abuse
- HIPAA permits disclosure about any individual believed to be a victim of abuse, neglect or domestic violence.
- 42 CFR Part 2 limits the exception to initial reports of child abuse or neglect (no other kinds of abuse or neglect).

Providers must follow 42 CFR Part 2, but if a state law compels to report other abuse:

- Obtain authorization
- Anonymous reporting
- QSO/BA with state agency
- Court order

Right to Access Records
- HIPAA REQUIRES a covered program to give an individual access to his/her own health information (with few exceptions).
- 42 CFR Part 2 gives programs DISCRETION to decide whether to permit patients to view or obtain copies of their records, unless they are governed by a state law that gives right to access.

Providers must follow HIPAA.
Privacy Notice

- HIPAA requires the Privacy Notice to be given at the time of first service.
- 42 CFR Part 2 requires the notice must be given at admission or as soon as a patient is capable of rational communication.

Providers must follow HIPAA.

Minimum Necessary

Under HIPAA, the standard of “Minimum Necessary” does not apply to uses or disclosures:

- to or by a health care provider for treatment
- made pursuant to a consent
- made to HHS for compliance and enforcement
- required by law
- Or required for compliance with the regulations

HOWEVER...

- 42 CFR Part 2 overrides these permissible exceptions to “Minimum Necessary”.

Providers must limit ALL DISCLOSURES to that information which is necessary to carry out the purpose of the disclosure (except to the patient him/herself).

AIDS/HIV

Uses and Disclosures

(410 ILCS 305/) AIDS Confidentiality Act

- Limiting the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish an intended purpose, when being transmitted by or on behalf of a covered entity under HIPAA, is a key component of health information privacy.
- The disclosure of HIV-related information, when allowed by this Act, shall be performed in accordance with the minimum necessary standard when required under HIPAA.

(Source: P.A. 98-1046, eff. 1-1-15.)

(410 ILCS 325/) Illinois Sexually Transmissible Disease Control Act

- Limiting the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish an intended purpose, when being transmitted by or on behalf of a covered entity under HIPAA, is a key component of health information privacy.
- The disclosure of HIV-related information, when allowed by this Act, shall be performed in accordance with the minimum necessary standard when required under HIPAA.

(Source: P.A. 98-1046, eff. 1-1-15.)
Sec. 8. Confidentiality. (Continued)

(c) A court hearing a request for the issuance of a warrant as authorized in subsection (c) of Section 6 of this Act shall conduct such proceedings in camera. A record shall be made of authorized proceedings but shall be sealed, impounded and preserved in the records of the court, to be made available to the reviewing court in the event of an appeal.

(d) No employee of the Department or its authorized representatives shall be examined in a civil, criminal, special or other proceeding concerning the existence or contents of pertinent records of a person examined or treated for a sexually transmissible disease by the Department or its authorized representatives pursuant to the provisions of this Act, or concerning the existence or contents of such reports received from a private physician or private health facility, pursuant to the provisions of this Act, without the consent of the person examined and treated for such diseases, except in proceedings under Sections 6 and 7 of this Act.

(e) Any person who knowingly violates the confidentiality provisions of this Section is guilty of a Class A misdemeanor.

(f) Any person who knowingly or maliciously disseminates any false information or report concerning the existence of any sexually transmissible disease under this Section is guilty of a Class A misdemeanor.

(Source: P.A. 89-381, eff. 8-18-95.)

IL Identity Protection Act

(5 ILCS 179/10)

- IL law requiring private businesses and government agencies to protect personally identifying information that could be used for identity theft. (For example: social security numbers)

- Includes specific actions private businesses and government agencies must take when experiencing a security breach involving personally identifying information that is not encrypted (not necessarily electronic encryption).

- Requires notifications of breaches to individuals, media, and IL Attorney General’s Office in specific situations.

Laws Protecting Specific Situations

Title X Family Planning: (45 CFR 59.11)

Federal law that requires providers to keep information about Title X Clients confidential and disclose it only with the client’s documented consent (permission), unless the disclosure is necessary to provide services to the client or is required by law.

Pharmacy Records Law

Availability of pharmacy records

- Pharmacy, whether written or electronic, orders are not public records and may only be provided to the following persons.
  - Persons for whom the prescription was written
  - Parent, Guardian or Persons standing in loco parentis of a minor child or disabled adult
  - Pharmacy owner & Pharmacist filling the prescription
  - Healthcare provider writing the prescription or otherwise treating the patient
Pharmacy Records Law
(List continued...)

- Anyone presenting an authorization for the release or subpoena for pharmacy information
- Includes researchers
- Any business entity responsible for paying for the medical care of the person for whom the prescription was written
- Pharmacy Board members
- HIPAA covered entity or non-covered health care provider for TPO purposes

Laws requiring disclosure

- Physicians must be report occupational injuries on farms and other reportable occupational diseases and illnesses to DHHS.
- Persons in charge of laboratories that provide diagnostic services must report findings related to reportable occupational diseases and illnesses to DHHS.

Other Exceptions Requiring Disclosure

Responding to a court order, subpoena, warrant, & other law enforcement and judicial requests:

- LHDs may disclose information without a patient’s permission upon receipt of a proper court order provided only the PHI disclosed is expressly authorized by the court order.
- A subpoena must never be ignored; however, depending on the type of subpoena, automatic disclosure of information is not always appropriate. (Consult the above guidance and local attorney.)

Health department should have a carefully crafted policy for handling subpoenas, court orders and law enforcement & judicial requests.

All the above requests should be brought to the attention of the health director immediately.

Consulting the LHD Attorney about the above types of legal requests prior to disclosing information is a good idea.

HIPAA’s effect on Public Health Scenarios

Scenario 1

- A family physician’s patient dies at home. The physician is asked to fill out a death certificate, which contains PHI as defined by the HIPAA privacy rule. Is this permitted without family authorization?
- Unauthorized disclosure is permitted. Vital statistics—required information on death and birth certificates—has not been changed by HIPAA. The information required on the death certificate can be provided without authorization.
HIPAA’s effect on Public Health Scenarios

Scenario 2
A patient is diagnosed with tuberculosis. This is a reportable disease per the state health code. Can the physician report the PHI requested on the disease reporting form?
Unauthorized disclosure is permitted. Each state health authority requires health care providers to report information about individuals who have contracted a disease of public health significance. Reportable disease lists differ by jurisdiction, and physicians should be aware of the diseases reportable in their areas and how the information is to be reported. Individual authorization for release of PHI in these disease reports is not required by HIPAA.

Scenario 3
A physician examines an infant who has unexplained injuries. Child abuse is suspected. Is child abuse reporting exempted from the privacy rule?
Unauthorized disclosure is permitted. Reporting of child abuse and neglect is exempted. This information may even be reported to a non-health agency, such as a child protective service, as long as the reportable information is required by law, and individual authorization is not required.

Scenario 4
A patient suffers what appears to be an adverse reaction to a medication. The FDA adverse event reporting form asks for PHI. Can a physician report PHI in this instance without patient authorization?
Unauthorized disclosure is permitted. Reporting of adverse events or reactions from drugs, food, biological products, and medical devices is still permitted without authorization.

Scenario 5
A patient is newly diagnosed with lung cancer. The state maintains a cancer registry and physicians are required to report PHI about patients with cancer. In this state the cancer registry is maintained by the university under contract with the State Health Department. Is reporting permitted without patient authorization?
Unauthorized disclosure is permitted. Cancer and immunization registry reporting of PHI is still permitted even if the entity responsible for the registry is not a public health agency, as long as it is under the authority of the agency to perform this public health function.

Scenario 6
A patient dies from meningitis and the local health department requests to view the hospital record to investigate cause of death. The cause turns out to be West Nile virus, which is not on the list of reportable diseases. Is the health department permitted to view the record and is authorization required?
Unauthorized disclosure is permitted. The privacy rule exception does not require a law or regulation specifically mandating disclosure. The health care provider can release requested information to a public health authority when the information is for the purpose of controlling disease, injury, or disability. The information released should be the minimum necessary for the stated public health purpose, and the provider can rely on the agency to determine what that information is. In this case, examination of the record is permitted and authorization is not required.

Scenario 7
An auditor from the Vaccine for Children program arrives at the office and requests to see patient records to audit adherence to the rules governing this program. Is the auditor allowed to exam records, and is authorization required?
Unauthorized disclosure is permitted. Patient records can be reviewed by staff of public health agencies authorized by law to collect PHI for program management purposes. No patient authorization is required.
HIPAA’s effect on Public Health Scenarios

• Scenario 8
  • A local community agency is concerned about the potential health effects of groundwater contamination. They request information about all your patients who have contracted cancer within the past 5 years. What information can you provide them?
  • PHI disclosure requires patient authorization. This agency, unless under the authority of a public health agency to collect PHI, cannot obtain PHI without patient authorization. However, deidentified information could be provided. Deidentified data are not covered by HIPAA and do not require individual privacy protection or authorization for release.

Is the HIPAA Privacy Rule suspended during a national or public health emergency?

• No; however, the Secretary of HHS may waive certain provisions of the Rule under the Project Bioshield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act.

• If the President declares an emergency or disaster and the Secretary declares a public health emergency, the Secretary may waive sanctions and penalties against a covered entity that does not comply with certain provisions of the HIPAA Privacy Rule:
  • the requirements to obtain a patient’s agreement to speak with family members or friends involved in the patient’s care (45 CFR 164.510(b))
  • the requirement to honor a request to opt out of the facility directory (45 CFR 164.510(a))
  • the requirement to distribute a notice of privacy practices (45 CFR 164.520)
  • the patient’s right to request privacy restrictions (45 CFR 164.522(a))
  • the patient’s right to request confidential communications (45 CFR 164.522(b))

Is the HIPAA Privacy Rule suspended during a national or public health emergency?

• Regardless of the activation of an emergency waiver, the HIPAA Privacy Rule permits disclosures for treatment purposes and certain disclosures to disaster relief organizations.
  • For instance, the Privacy Rule allows covered entities to share patient information with the American Red Cross so it can notify family members of the patient’s location. See 45 CFR 164.510(b)(4).

Illinois Confidentiality Laws

• There are extensive laws that apply to Illinois providers, payors, and others, establishing rights and obligations with respect to maintaining patient privacy, and confidentiality and security of patient health information.
  • These laws drive health information exchange practices in Illinois and should be taken into account.
Illinois Confidentiality Laws

- AIDS Confidentiality Act, 410 ILCS 305/1 et seq.
- Alcoholism and other Drug Abuse and Dependency Act, 20 ILCS 301/1 et seq.
- Child Care Act of 1969, 225 ILCS 10/1 et seq. (applicable to childcare facilities).
- Genetic Information Privacy Act, 410 ILCS 513/1 et seq.
- Dental Care Patient Protection Act, 215 ILCS 109/1 et seq. (a patient has the right to privacy and confidentiality).
- Early Intervention Services System Act, 325 ILCS 20/1 et seq.
- Early Intervention Services System Act Regulations:
  - Rules Implementing the Early Intervention Services System Act, 89 Ill. Adm. Code 500.155
  - (written consent regarding use and exchange of information).
- Hospital Licensing Act, 210 ILCS 87/6.17 (protection of and confidential access to medical records and information).
- Hospital Licensing Regulations, 77 Ill. Adm. Code 300.1800 (Resident Record Requirements), 300.4320 (Confidentiality of Resident’s Records).

Illinois Confidentiality Laws

- Hospital Licensing Act, 210 ILCS 87/6.17 (protection of and confidential access to medical records and information).
- Illinois Public Aid Code, 305 ILCS 5/1 et seq. (confidentiality and protection of records)
  - (standards for collection, use and disclosure of information gathered by insurers in connection with life, health, disability, property and casualty insurance transactions), including Article XLI (Insurance Information and Privacy Protection), 215 ILCS 5/1001 et seq. (standards for the collection, use and disclosure of information gathered in connection with insurance transactions, including medical record information, and restrictions on disclosures without patient authorization and required form of authorization).
- Managed Care Reform and Illinois Patient’s Rights Act, 215 ILCS 134/1 et seq. (Right to privacy and confidentiality in health care.)
- Medical Patient Rights Act, 410 ILCS 50/0.01 et seq. (Patient’s right to privacy and confidentiality of records, including restrictions on disclosures by physicians, health care providers, health services corporations and insurance companies.)
- Medicare Conditions of Participation for Hospitals, 42 CFR 482.13 (Patient’s right to personal privacy and confidentiality of clinical records).

Illinois Confidentiality Laws

- Illinois Constitution, Article I, Section 6 (right to privacy)
Illinois Confidentiality Laws

- Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/1 et seq.
- Workers’ Compensation Act, 820 ILCS 305/1 et seq.

Federal Confidentiality Laws

The laws addressing the mandatory and permissive reporting obligations of health care providers and others in Illinois contain confidentiality protections and limitations on the release of patient information, such as is provided in the following:

- Abused and Neglected Child Reporting Act, 325 ILCS 5 et seq.
- Child Sexual Abuse Prevention Act, 325 ILCS 15 et seq.
- Communicable Disease Report Act, 745 ILCS 45/0.01 et seq.
- Control of Sexually Transmissible Diseases Code, 77 Ill. Adm. Code 693.100.
- Domestic Abuse of Disabled Adults Intervention Act, 20 ILCS 2435 et seq.

Federal Confidentiality Laws

(Special Protections for Research Uses and Disclosures)

- Department of Health and Human Services, Public Welfare, “Common Rule” Regulations, 45 CFR Part 46 (regulations for research involving human subjects conducted, supported or otherwise subject to regulation by federal agencies).
- Food and Drug Administration, Department of Health and Human Services “Protection of Human Subjects” Regulations, 21 CFR Part 50 (regulations applicable to all clinical investigations regulated by the FDA and clinical investigations supporting applications for research or marketing permits for products regulated by the FDA).

Know how to protect PHI/ePHI with compliance activities
Key Components of Compliance with Privacy Rule
- Policies and procedures
- Privacy Officer
- Training Program
- Complaint Process
- Internal compliance audit program
- Sanctions
- Incident response and corrective action procedures

Suggested Next Steps
- Perform HIPAA compliance assessments
  - High level review
- Conduct/Review HIPAA IT Security Risk Analysis
  - Detail level review
- Provide HIPAA education
  - Annual basis
  - New Hire Orientation
- When PHI/ePHI is used, disclosed, and accessed
- Develop policies and procedures that contain HIPAA enforcement
  - Performance Improvement Plan

Suggested Next Steps (Continued)
- Perform PHI/ePHI inventory
- Update Notice of Privacy Practices
- Review and identify all Business Associates
- Update Business Associate Agreements
- Update breach notification policies and procedures
- Develop and train employees on new policies (patient requested PHI restrictions, patient requested electronic copies of PHI, breach notification, etc)
- Review and update authorization and other forms as necessary

Bottom Line
- HIPAA, ARRA, HITECH are the law
- There are civil and criminal penalties for non-compliance
- Affects all and requires cooperation
- HIPAA, ARRA, HITECH are not simply "IT" issues–they have implications for your entire organization
- Could have major impact on operations and reimbursement
- Has impact on future business strategies