Illinois Health and Hospital Association

HIPAA, BIPA, GIPA, and PIPA – OH MY! An Update on Regulations Affecting Patient Privacy

Michael A. Woods
Assistant Vice President and Deputy General Counsel
September 20, 2024

This session is presented for informational and educational purposes only. Nothing in this session should be construed as legal advice or an offer of representation. The presentation is not a substitute for independent professional judgment or legal advice concerning the law as applied to a particular situation or matter.

What is the data that is protected by HIPAA, BIPA, GIPA, and PIPA?

What types of requests for PHI concerning reproductive health are prohibited under HIPAA?

What kind of informed consent is needed for “sensitive” examinations?

Illinois Health and Hospital Association

HIPAA Privacy Rule

A covered entity may not use or disclose PHI, except either:

- As the Privacy Rule *requires* or *permits*; or
- As the individual who is the subject of the information (or the individual's personal representative) authorizes in writing (unless *prohibited*).

What is PHI?

- All "***individually identifiable health information***" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

- "***Individually identifiable health information***" is information, including demographic data, that relates to: (1) the individual's past, present or future physical or mental health or condition, (2) the provision of health care to the individual, or (3) the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

HIPAA Required Disclosures

The Privacy Rule Requires Disclosures (45 CFR 164.502(a)(2))

- To the Individual under their right to access and for an accounting of disclosures.
- HHS review, compliance, investigation and enforcement.

HIPAA Permitted Disclosures

The Privacy Rule Permits Uses and Disclosures (45 CFR 164.502(a)(1))

- To the Individual.
- Treatment, Payment, and Healthcare Operations (164.506).
- Incident to an otherwise permitted Use and Disclosure (when in compliance with 164.502(b) & 164.514(d) (min necessary), and 164.530(c) (safeguards)).
- In compliance with a valid authorization (unless prohibited) (164.508).
- Opportunity to agree or object (e.g., facility directories, individuals involved in care, notification to individuals, disaster relief, if the individual is deceased) (164.510).
- Limited Data Set for the purposes of Research, Public Health, or Health Care Operations (164.514(e)).
- Fundraising Communications (164.514(f)).
- Underwriting (unless prohibited) (164.514(g)).
- Public interest and benefit activities (164.512 and, where applicable 164.509).

HIPAA Permitted Disclosures (continued)

Public Interest and Benefit Activities

- Disclosures required (not permitted) by law (e.g., federal, state, or local) (164.512(a)).
- Public health activities (e.g., surveillance or investigations) (e.g., (164.512(b)).
- Victims of abuse, neglect or domestic violence (excludes child abuse/neglect) (164.512(c)).
- Health oversight activities (e.g., authority to oversee) (164.512(d),164.509 applies).
- Judicial and administrative proceedings (e.g., subpoenas) (164.512(e),164.509 applies).
- Law enforcement purposes (e.g., process, ID/location, victims, death, crime on premises, crime in emergencies) (164.512(f),164.509 applies).
- Decedents (164.512(g))
  - Coroners and Medical Examiners (164.512(g)(1),164.509 applies).
  - Funeral Directors (164.512(g)(2)).
- Cadaveric Organ, Eye, or Tissue Donation (e.g., OPOs) (164.512(h)).
- Research (164.512(i)).
- Serious Threat to Health or Safety (e.g., “duty to warn”) (164.512(j)).
- Specialized government functions (e.g., military, national security, secret service) (164.512(k)).
- Worker’s compensation (to the extent necessary to comply with laws relating to workers' compensation) (164.512(l)).

HIPAA Prohibited Disclosures

The Privacy Rule <u>Prohibits</u> Uses and Disclosures (45 CFR 164.502(a)(5))

- Of genetic information for underwriting purposes (164.502(a)(5)(i)).
- For the sale of protected health information (164.502(a)(5)(ii)).
- To conduct, impose, or identify any person for the purpose of conducting a criminal, civil, or administrative investigation for the mere act of seeking, obtaining, providing, or facilitating reproductive health care (164.502(a)(5)(iii)).

Why isn't HIPAA the only thing?

Supremacy Clause (Article VI, Clause 2) provides that the Constitution and the laws and treaties made pursuant to it, shall be the supreme law of the land.

HIPAA has holes.

Definitional Exclusions

- ***Protected Health Information*** excludes "individually identifiable health information" in:
  - In records covered by the Family Educational Rights and Privacy Act (FERPA).
  - Employment records held by a covered entity in its capacity as an employer.
  - A person that has been deceased for >50 years.

Preemption and Exemptions 45 C.F.R. 160.203

- State laws that are *contrary* to the Privacy Rule are preempted unless an *exception* applies.

Is the state law preempted?

Step 1: Is the state law "contrary" to a HIPAA requirement?

- Contrary means, in part, that a covered entity or business associate would find it impossible to comply with both the state and federal requirements.

State Law	HIPAA	Covered Entity
Permits Disclosure	Prohibits Disclosure (3x)	Nondisclosure complies with both.
Permits Disclosure	Mandates Disclosure (2x)	Disclosure complies with both.
Prohibits Disclosure	Permits Disclosure (20x)	Nondisclosure complies with both.
Prohibits Disclosure	Mandates Disclosure (2x)	CANNOT COMPLY WITH BOTH – Preemption unless exception.
Mandates Disclosure	Permits Disclosure (20x)	Disclosure complies with both.
Mandates Disclosure	Prohibits Disclosure (3x)	CANNOT COMPLY WITH BOTH – Preemption unless exception.

- If the state law, HIPAA, or both are permissive the state law will not be contrary.

Is the state law preempted?

Step 2: Does an exception apply?

- Exceptions:
  - (1) An HHS Secretary determination;
  - (2) The state law relates to the privacy of individually identifiable health information and is more stringent (i.e., provides greater privacy protections or privacy rights with respect to such information) than HIPAA;
  - (3) The state law provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention; or
  - (4) The state law requires certain health plan reporting, such as for management or financial audits.

Biometric Information Privacy Act (BIPA)

Data Protected: Biometric Identifiers & Information

- ***Biometric Identifier*** means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Excludes:
  - Writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions.
  - Donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act….
  - Biological materials regulated under GIPA.
  - **Information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.**
  - An X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film.

- ***Biometric Information*** means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Excludes: information derived from items or procedures excluded under Biometric Identifiers.

Biometric Information Privacy Act (BIPA)

Pre-Collection Requirements:

- Prior to collection you must: (1) inform the individual in writing that a biometric identifier or biometric information is being collected or stored; (2) inform the individual in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receive a signed written release consenting to the collection.

Pre-Disclosure Requirements:

- Disclosure prohibited unless: (1) the individual consents to the disclosure; (2) the disclosure completes a financial transaction authorized by the individual; or (3) the disclosure is required to comply with State or federal law, municipal ordinance, or (4) pursuant to a valid warrant or subpoena.

General Requirements:

- Written publicly available policy.
- Reasonable security measures.

Biometric Information Privacy Act (BIPA)

A private right of action for individuals "aggrieved" by a violation.

Bad for Hospitals:

- *Rosenbach v. Six Flags Entertainment Corp.* (2019) held that individuals do not need to allege any "actual injury or adverse effect," beyond simply demonstrating a violation of the law.
- *Tims v. Blackhours Carriers, Inc.* (2023), the Court rejected a one-year statute of limitations for claims under BIPA, ruling instead that a five-year statute of limitations applies to these cases.
- *Cothron v. White Castle* (2023) held that every violation is considered a separate offense, ruling a claim arises each time the data is collected, rather than just the first time.

Good for Hospitals:

- *Mosby v. The Ingalls Memorial Hospital* (2023) the Court ruled that a healthcare provider's collection of finger-scan information from its employees is not "biometric information" as defined by BIPA when such information is used for "treatment," "payment," or "health care operations" as defined by HIPAA.
- Public Act 103-0769: amends BIPA to clarify that any person whose biometric identifier or biometric information is "scanned" by a private entity (regardless of its frequency) may only recover damages for one violation (overturns *Cothron*).

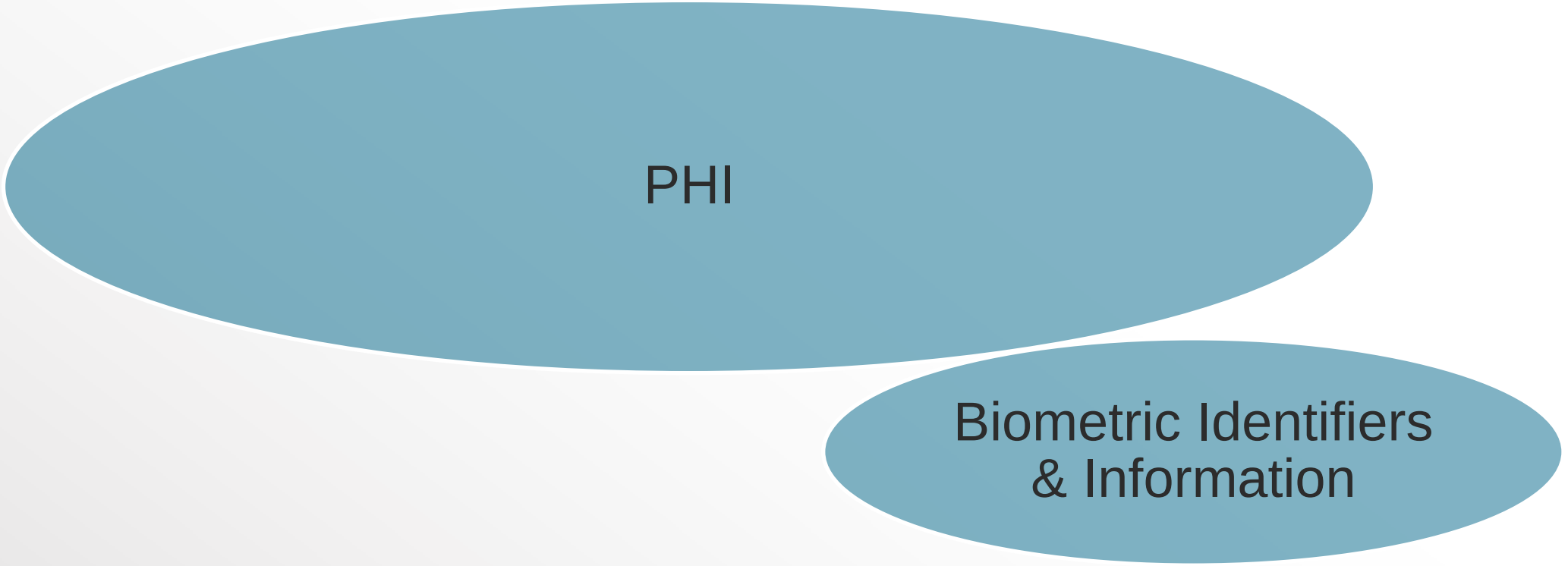
Biometric Information Privacy Act (BIPA)

Does HIPAA apply?

- Patient or employee records? Employment records held by a covered entity in its capacity as an employer is not PHI.
- BIPA excludes information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

Does HIPAA Preempt BIPA?

- They are mutually exclusive.


PHI
Biometric Identifiers
& Information

Genetic Information Privacy Act (GIPA)

Data Protected: Genetic Information (as defined by HIPAA)

- ***Genetic Information*** means information about an individual's genetic tests; the genetic tests of family members of the individual; the manifestation of a disease or disorder in family members of such individual; or any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. Includes the genetic information concerning a fetus carried by the individual or family member who is a pregnant woman and any embryo legally held by an individual or family member utilizing an assisted reproductive technology. Excludes information about the sex or age of any individual.

- ***Genetic Test*** means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Genetic Information Privacy Act (GIPA)

Pre-Collection Requirements:

- A health care provider, health care professional, or health facility who ordered the genetic test shall make a reasonable effort to notify the minor's parent or legal guardian, if, in their professional judgment notification would be in the best interest of the minor and they have first sought unsuccessfully to persuade the minor to notify the parent or legal guardian or after a reasonable time after the minor has agreed to notify the parent or legal guardian, they have reason to believe that the minor has not made the notification (no duty is created).

Genetic Information Privacy Act (GIPA)

Pre-Disclosure Requirements and Exceptions:

- Except as otherwise provided, genetic testing and information derived from genetic testing is confidential and privileged and may be released only to the individual tested and to persons specifically authorized, in writing in accordance with Section 30, by that individual to receive the information.
  - Section 30. No person may disclose or be compelled to disclose the identity of any person upon whom a genetic test is performed or the results of a genetic test in a manner that permits identification of the subject of the test except to:
    - The subject of the test or their legal representative or those designated in a specific written legally effective authorization.
    - An agent or employee of a health care facility or health care provider (if authorized to obtain or have results) for patient care.
    - A health care facility or health care provider that procures, processes, distributes, or uses a human body part.
    - Health facility staff committees for quality review.
- Exceptions Otherwise Provided.
  - A covered entity may, without consent, use and disclose genetic information for treatment, payment, and health care operations (410 ILCS 513/31).
  - A covered entity may, without consent, use and disclose genetic information for health oversight activities (410 ILCS 513/31.1).
  - May disclose, without consent, for public health activities ((410 ILCS 513/31.2).
  - A covered entity may, without consent, disclose genetic information to a business associate (410 ILCS 513/31.3).
  - Disclosure of information from a patient's record to law enforcement or for law enforcement purposes (410 ILCS 513/31.6).
  - A covered entity may, without consent, use and disclose genetic information to create a limited data set or de-identify (410 ILCS 513/31.7).
  - May disclose for research in accordance with HIPAA (410 ILCS 513/31.9).

Genetic Information Privacy Act (GIPA)

Employer Prohibitions:

- Must treat genetic testing and genetic information consistent with existing nondiscrimination laws (e.g., the Genetic Information Nondiscrimination Act of 2008, ADA, etc.).
- May not:
  - Condition employment on genetic testing.
  - Affect the terms, conditions, or privileges of employment because of a genetic test.
  - Limit, segregate, or classify employees adversely because of a genetic test.
  - Retaliate against any person alleging a violation of GIPA.
- May not offer pay or benefits in return for taking a genetic test.
- May not use genetic information or testing in furtherance of a wellness program unless it meets certain conditions.

Genetic Information Privacy Act (GIPA)

A private right of action for individuals "aggrieved" by a violation.

Sound familiar?

- Capitalizing on the success of BIPA lawsuits, trial attorneys have begun to use the same theories they used under BIPA to bring similar lawsuits under GIPA.
- Over an eight-month period last year, at least 20 class action lawsuits were filed. In comparison, only two GIPA lawsuits were filed in all of 2021 and no cases were filed in 2022.
- The common theme in these lawsuits are allegations that employers requested or required job candidates, as part of their pre-employment physical examination, to disclose their family medical histories before receiving employment offers. Plaintiffs allege that these questions led to their disclosure of genetic information as a condition of employment, in violation of GIPA.
- Using the same argument that they used in BIPA – that no actual harm needs to occur – trial attorneys claimed that under GIPA the statutes' penalties should apply.

Genetic Information Privacy Act (GIPA)

In the absence of legislative action, review your current policies and practices and implement protective actions such as:

- Advising third-party medical providers performing employee screenings to modify their procedures and not ask employees about family medical history.
- Consider updating the indemnification obligations in contracts with such third-party medical providers.
- Consider adding a disclaimer to post-offer and pre-employment questionnaires that asks prospective employees not to provide any genetic information when responding to requests for medical information.

Genetic Information Privacy Act (GIPA)

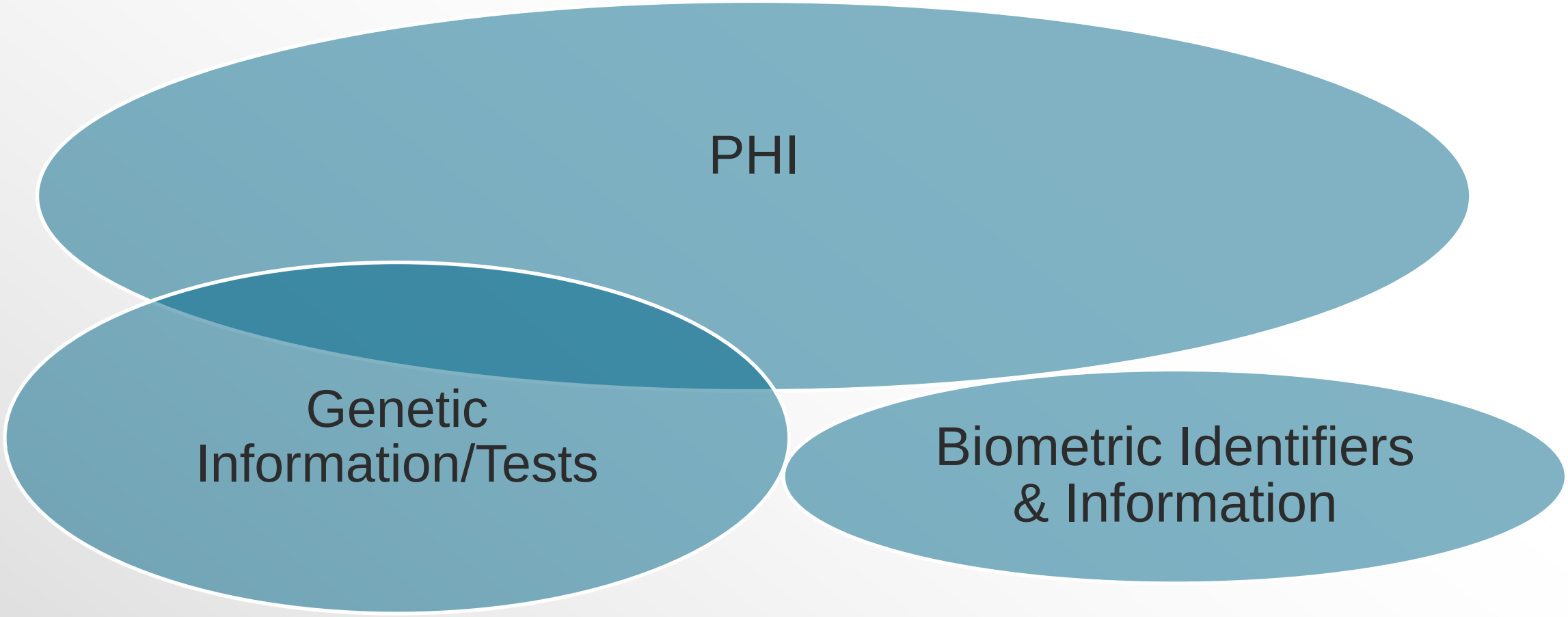
Does HIPAA apply?

- Patient or employee records? Employment records held by a covered entity in its capacity as an employer is not PHI.

Does HIPAA Preempt GIPA?

- No, GIPA does not prohibit disclosure when HIPAA mandates it, nor does it mandate disclosure when HIPAA prohibits it.

State Law	HIPAA	GIPA	Covered Entity
Permits Disclosure	Prohibits Disclosure (3x)	Yes	Nondisclosure complies with both.
Permits Disclosure	Mandates Disclosure (2x)	Yes	Disclosure complies with both.
Prohibits Disclosure	Permits Disclosure (20x)	Yes	Nondisclosure complies with both.
Prohibits Disclosure	Mandates Disclosure (2x)	No	Preemption unless exception.
Mandates Disclosure	Permits Disclosure (20x)	NA	Disclosure complies with both.
Mandates Disclosure	Prohibits Disclosure (3x)	NA	Preemption unless exception.


PHI
Genetic Information/Tests
Biometric Identifiers & Information

Personal Information Protection Act (PIPA)

Data Protected: Personal Information

Personal information means either of the following:

- An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:
  - Social Security number.
  - Driver's license number or State identification card number.
  - Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
  - Medical information.
  - Health insurance information.
  - Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
- User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

Personal Information Protection Act (PIPA)

General Requirements

- Notice of Breach
  - Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach.
  - Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person and cooperate in accordance with the PIPA.
- Disposal of Personal Information
  - A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable.
- Data Security
  - A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.
  - A contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

Personal Information Protection Act (PIPA)

Exemption

- Section 50. Entities subject to the federal Health Insurance Portability and Accountability Act of 1996. Any covered entity or business associate that is subject to and in compliance with the privacy and security standards for the protection of electronic health information established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act *shall be deemed to be in compliance with the provisions of this Act, provided that any covered entity or business associate required to provide notification of a breach to the Secretary of Health and Human Services pursuant to the Health Information Technology for Economic and Clinical Health Act also provides such notification to the Attorney General within 5 business days of notifying the Secretary*.

Personal Information Protection Act (PIPA)

Violations are an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act

- Attorney General or State's Attorney may request a civil penalty in a sum not to exceed $50,000.
- Consumers may be able to recover actual and punitive damages as well as attorney's fees and costs, and injunctive relief.

Civil Penalties for Improper Disposal of Personal Information

- $100 for each individual's information disposed of in violation up to $50,000.

Personal Information Protection Act (PIPA)

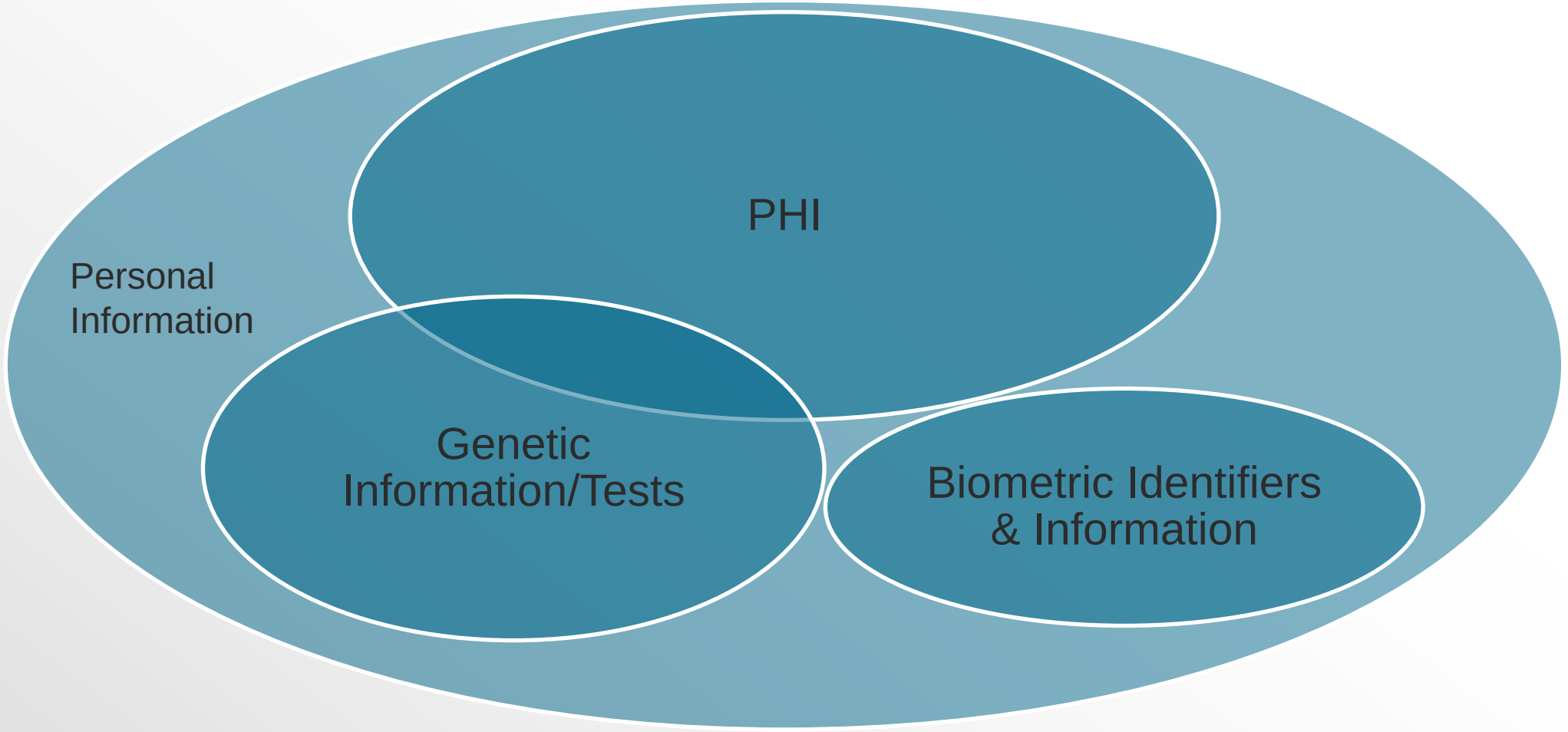
Does HIPAA apply?

- Patient or employee records? Employment records held by a covered entity in its capacity as an employer is not PHI.

Does HIPAA Preempt PIPA?

- No, PIPA does not prohibit disclosure when HIPAA mandates it, nor does it mandate disclosure when HIPAA prohibits it.

State Law	HIPAA	PIPA	Covered Entity
Permits Disclosure	Prohibits Disclosure (3x)	NA	Nondisclosure complies with both.
Permits Disclosure	Mandates Disclosure (2x)	NA	Disclosure complies with both.
Prohibits Disclosure	Permits Disclosure (20x)	NA	Nondisclosure complies with both.
Prohibits Disclosure	Mandates Disclosure (2x)	NA	Preemption unless exception.
Mandates Disclosure	Permits Disclosure (20x)	NA	Disclosure complies with both.
Mandates Disclosure	Prohibits Disclosure (3x)	NA	Preemption unless exception.


Personal
Information
PHI
Genetic
Information/Tests
Biometric Identifiers
& Information

It’s a Minefield

- **HIPAA Administrative Simplification Regulations, 45 CFR Parts 160, 162, and 164.**
- **Biometric Information Privacy Act (BIPA), 740 ILCS 14/1 et seq.**
- **Genetic Information Privacy Act (GIPA), 410 ILCS 513/1 et seq.**
- **Personal Information Protection Act (PIPA), 815 ILCS 530/1 et seq.**
- Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/1 et seq.
- AIDS Confidentiality Act, 410 ILCS 305/1 et seq.
- Alcoholism and other Drug Abuse and Dependency Act, 20 ILCS 301/1 et seq.
- Confidentiality of Alcohol and Drug Abuse Records, 42 CFR Part 2.
- Hospital Licensing Act, 210 ILCS 85/6.17; Hospital Licensing Regulations, 77 Ill. Adm. Code 250.1510.
- Illinois Constitution, Article I, Section 6.
- Illinois Public Aid Code, 305 ILCS 5/1-1 et seq.
- Managed Care Reform and Illinois Patient’s Rights Act, 215 ILCS 134/1 et seq.
- Medical Patient Rights Act, 410 ILCS 50/0.01 et seq.
- Medicare Conditions of Participation for Hospitals, 42 CFR 482.13 .
- Physician and Patient Privilege, 735 ILCS 5/8-101.

Navigating the Minefield

First, focus on the "what" - the thing or things that need to be disclosed.

- What type of data do you want to disclose or is being requested to be disclosed?
- Is it patient data, employee data, or both?
- Does the data contain information protected by different laws?
- The key - having a working knowledge on the type of data protected by different laws.

Then, focus on the "how" – can it be disclosed?

- What is required, permitted, or prohibited?
- Does the proposed disclosure meet the conditions in the law(s) about who, when, where, and why?
- The key – reading the law.

HIPAA Reproductive Health Care Final Rule Overview

A covered entity or business associate may not use or disclose protected health information for any of the following activities:

- To conduct a criminal, civil, or administrative investigation or impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care.
- To identify any person for the purpose of conducting the investigation or imposing liability (164.502(a)(5)(iii)).

"Reproductive Health Care" is broadly defined:

Reproductive Health Care means "***Health Care***," as defined by HIPAA, that affects the health of the individual in all matters relating to the reproductive system and to its functions and processes. This definition shall not be construed to set forth a standard of care for or regulate what constitutes clinically appropriate reproductive health care (160.103)

HIPAA Reproductive Health Care Final Rule Overview

The prohibition on disclosure only applies if the relevant activity is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care, and the covered entity has reasonably determined the existence of one or more of the following:

(1) The reproductive health care is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided.

(2) The reproductive health care is protected, required, or authorized by Federal law, including the United States Constitution, under the circumstances in which such health care is provided, regardless of the state in which it is provided.

(3) The presumption applies (when the covered entity did not provide the reproductive health care at issue): The reproductive health care provided by another covered entity is presumed lawful unless the covered entity has:

- Actual knowledge that the reproductive health care was not lawful under the circumstances in which it was provided.
- Factual information supplied by the person requesting the PHI that demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided (164.502(a)(5)(iii)(B) & (C)).

HIPAA Reproductive Health Care Final Rule Overview

Permitted disclosures for the following purposes:

- **Health oversight activities (164.512(d)).**
- **Judicial and administrative proceedings (164.512(e)).**
- **Law enforcement purposes (164.512(f)).**
- **Coroners and Medical Examiners (164.512(g)(1)).**

Now require a covered entity to obtain a *valid* attestation from the requestor that the PHI will not be used for a prohibited purpose prior to disclosure of PHI potentially related to reproductive health care. Reliance on a *defective* attestation is not compliant with the attestation requirement (164.509).

The rule includes what constitutes a valid attestation as well as a defective attestation.

HIPAA Reproductive Health Care Final Rule Overview

What about permitted disclosures for public health purposes?

- New definition of “public health”
- ***Public Health*** as used in the terms “public health surveillance,” “public health investigation,” and “public health intervention,” means population-level activities to prevent disease in and promote the health of populations…But such activities do not include those with any of the following purposes: [repeats reproductive disclosure prohibitions].
- Prevents backdoor requests to avoid attestation required requests.
- Limits one of HIPAA’s preemption limitations. HIPAA does not preempt laws providing for “…the conduct of public health surveillance, investigations, or interventions.” The definition anticipates the use of public health laws to circumvent the application of the prohibition.

HIPAA Reproductive Health Care Final Rule Overview

Important Dates:

- **Compliance with the rule except the Notice of Privacy Practices is December 23, 2024.**
- **Compliance with the Notice of Privacy Practices February 16, 2026**
- **HHS does intend to release a model attestation prior to December 23, 2024.**

Informed Consent for “Sensitive” Examinations.

- On April 1, 2024, CMS revised its Hospital Interpretive Guidelines in its State Operations Manual, Appendix A at tag A-0955.

- Tag A-0955 begins the interpretive guidelines for Medicare COP 42 CFR 482.51(b)(2): A properly executed informed consent form for the operation must be in the patient’s chart before surgery, except in emergencies.

- The guidance discusses the requirements for a hospital’s surgical informed consent policy and an example of a well-designed informed consent process.

- Within the example of a well-designed informed consent process, clarifies that it should include discussion of whether residents, medical, advanced practice provider (such as nurse practitioners and physician assistants) and other applicable students, will be performing “examinations or invasive procedures for educational and training purposes.”

- Examinations or invasive procedures conducted for educational and training purposes include breast, pelvic, prostate, and rectal examinations, as well as those specified under state law.

Informed Consent for “Sensitive” Examinations.

Under “Example of a Well-Designed Informed Consent Process,” CMS added:

Whether physicians other than the operating practitioner, including, but not limited to, residents, *medical, advanced practice provider (such as nurse practitioners and physician assistants), and other applicable students*, will be performing important tasks related to the surgery, *or examinations or invasive procedures for educational and training purposes,* in accordance with the hospital’s policies. Important surgical tasks include: opening and closing, dissecting tissue, removing tissue, harvesting grafts, transplanting tissue, administering anesthesia, implanting devices, and placing invasive lines. *Examinations or invasive procedures conducted for educational and training purposes include, but are not limited to, breast, pelvic, prostate, and rectal examinations, as well as others specified under state law*.

Informed Consent for “Sensitive” Examinations.

What does Illinois law say?

Medical Patient Rights Act (410 ILCS 50/7)

Patient examination. Any physician, medical student, resident, advanced practice registered nurse, registered nurse, or physician assistant who provides treatment or care to a patient shall inform the patient of his or her profession upon providing the treatment or care, which includes but is not limited to any physical examination, such as a pelvic examination. In the case of an unconscious patient, any care or treatment must be related to the patient's illness, condition, or disease. (Source: P.A. 100-513, eff. 1-1-18.)

Informed Consent for “Sensitive” Examinations.

Requirements:

- Examinations or invasive procedures conducted for educational and training purposes (“sensitive” examinations) performed in the context of surgery, especially those involving anesthesia, must be performed pursuant to informed consent (i.e., a reference to the use/involvement of residents in a general consent to treatment is insufficient). This will most likely be captured through an informed consent form – the same or separate from the surgical consent - rather than only documentation in the medical record.
- Any policy regarding “sensitive” examinations must address Illinois law’s limitation that any sensitive exam performed on a patient under anesthesia must be related to the patient's illness, condition, or disease (e.g., routinely performed).

Informed Consent for “Sensitive” Examinations.

Recommendations:

- All “sensitive” examinations should be done pursuant to specific consent and preferably documented by a separate, written informed consent form even when not required by federal or state law.
- All “sensitive” examinations should be limit to instances in which such examinations are standard, routine practice.

Michael A. Woods | Assistant Vice President & Deputy General Counsel
T 630.276.5627 | mwoods@team-iha.org | www.team-iha.org
Illinois Health and Hospital Association
1151 E. Warrenville Road, Naperville, IL 60563

Illinois Health and Hospital Association

Your trusted voice and resource

team-iha.org

HIPAA
Protected Health Information

- Means all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- "Individually identifiable health information" is information, including demographic data, that relates to: (1) the individual's past, present or future physical or mental health or condition, (2) the provision of health care to the individual, or (3) the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
- **The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g.**

PIPA
Personal Information

- An individual's first name or first initial and last name in combination with any one or more of the following data elements (when not encrypted/redacted or the keys to unencrypt/unredact have been acquired through a breach): (1) Social Security #, (2) driver's license # or state identification card #, (3) account # or credit or debit card #, or an account # or credit card # in combination with any required security code, access code, or password that would permit access to an individual's financial account, (4) medical information, (5) health insurance information, or (5) unique biometric data (i.e., measurements or technical analysis of human body characteristics – e.g., fingerprint, retina or iris image).
- User name or email address with a password or security question and answer (when not encrypted/redacted or the keys to unencrypt/unredact have been acquired through a breach).
- PIPA excludes publicly available information that is lawfully made available to the general public from federal, State, or local government records from “Personal Information.”
- Compliance with HIPAA = compliance with PIPA (notification to AG still required) 815 ILCS 530/50.

BIPA
Biometric Identifiers & Information

- Biometric Identifier means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

- Biometric identifiers do not include:
  - Writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions.
  - Donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act….
  - Biological materials regulated under GIPA.
  - **Information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.**
  - An X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film.

- Biometric Information means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

- Biometric Information does not include information derived from items or procedures excluded under Biometric Identifiers.

GIPA
Genetic Testing & Information

- Refers to definitions under HIPAA at 45 CFR 160.103.

- Genetic Testing (including direct-to-consumer testing) means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes.

- Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition. .

- “Genetic Information” means: (1) the individual's (including a fetus or embryo) genetic tests, (2) the genetic tests of family members of the individual, (3) the manifestation of a disease or disorder in family members of such individual; or (4) any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

- Genetic information excludes the sex or age of any individual.

BIPA, GIPA, PIPA and HIPAA Comparison Chart

	State Law	HIPAA	Applicability	Covered Entity
BIPA	Mutually Exclusive	Mutually Exclusive	NA	BIPA and HIPAA are mutually exclusive.
GIPA	Permits Disclosure	Prohibits Disclosure (3x)	Yes	Nondisclosure complies with both.
	Permits Disclosure	Mandates Disclosure (2x)	Yes	Disclosure complies with both.
	Prohibits Disclosure	Permits Disclosure (20x)	Yes	Nondisclosure complies with both.
	Prohibits Disclosure	Mandates Disclosure (2x)	No	Preemption unless exception.
	Mandates Disclosure	Permits Disclosure (20x)	NA	Disclosure complies with both.
	Mandates Disclosure	Prohibits Disclosure (3x)	NA	Preemption unless exception.
PIPA	Permits Disclosure	Prohibits Disclosure (3x)	NA	Nondisclosure complies with both.
	Permits Disclosure	Mandates Disclosure (2x)	NA	Disclosure complies with both.
	Prohibits Disclosure	Permits Disclosure (20x)	NA	Nondisclosure complies with both.
	Prohibits Disclosure	Mandates Disclosure (2x)	NA	Preemption unless exception.
	Mandates Disclosure	Permits Disclosure (20x)	NA	Disclosure complies with both.
	Mandates Disclosure	Prohibits Disclosure (3x)	NA	Preemption unless exception.