EPSTEIN BECKER GREEN

What's Ahead in Data Privacy and Security Issues

Allen Killworth **Lisa Pierce Reisz**

Ohio Hospital Association Annual Meeting

May 20, 2026

Agenda

- Introduction
- HIPAA (Old) Proposed Rules
- Part 2 and (Vacated) RHI Rule
- Minor Records
- Enforcement Issues
- CIRCIA Proposed Rule
- SECURE Act
- AI Issues
- Questions

EPSTEIN
BECKER
GREEN

HIPAA
Proposed Rules – New Life for These Old Rules?

Proposed Security Rule Revisions

- HIPAA *Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information* published January 6, 2025. See: https://www.ebglaw.com/insights/publications/proposed-hipaa-security-rule-updates-may-significantly-impact-covered-entities-and-business-associates

Key provisions include:

- New/Updated Definitions
- Addressable vs. Required
  - Proposed Rule would remove the distinction between "addressable" and "required" specifications, making **all** implementation specifications required, except for a few narrow exemptions.
- Changes to Risk Analysis
  - Proposed Rule would impose specific requirements to be included in a risk analysis and require that risk analyses be reviewed, verified, and updated at least once every 12 months or in response to environmental or operational changes impacting ePHI.
- Technology Asset Inventories & Network Maps
  - Proposed Rule would imposed explicit requirements to create a technology asset inventory and a network map and require these to be reviewed and updated at least once every 12 months.

Proposed Security Rule Revisions

- Verifying BA Compliance
  - Proposed Rule would require CEs to obtain written verification of the technical safeguards used by BAs that create, maintain, or transmit ePHI on their behalf at least every 12 months.
- Patch Management
  - Proposed Rule would create a new patch management standard requiring CEs/BAs to implement policies and procedures for identifying, prioritizing, and applying software patches throughout their relevant electronic information systems, including specific timing requirements based on the criticality of the patch in question.
- Workforce Controls
  - Proposed Rule would establish more explicit requirements for workforce control policies, which must be written and reviewed at least once every 12 months. Proposed Rule would impose specific timing requirements for workforce access and training.
- Technical Safeguards
  - Proposed Rule would establish Minimum Technical Safeguards including requirement that CEs/BAs use multi-factor authentication requirements that are consistent with the CPGs.
- Contingency/Disaster Planning
  - Proposed Rule would add obligations relative to contingency planning, including requirements to identify critical electronic information systems, and establish relatively short timing requirements for implementation of procedures and notification of CEs by BAs of activation of contingency plans.

Proposed Privacy Rule Revisions

- HIPAA *Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement* published January 21, 2021.
- HHS stated that the revisions would "address standards that may impede the transition to value-based health care by limiting or discouraging care coordination and case management communications among individuals and covered entities (including hospitals, physicians, and other health care providers, payors, and insurers) or posing other unnecessary burdens."

Proposed Privacy Rule Revisions

Key provisions

- **Right of Access**
  - Timeframe to respond to individual's request would be *reduced* to not later than 15 calendar days (currently 30 days) with possibility to extend period no more than 15 calendar days (currently a 30 days).
  - Identity verification of individuals requesting access would be *reduced* to prohibit a covered entity from imposing unreasonable identity verification measures on an individual (or his or her personal representative).
  - Right to inspect PHI in person would be strengthened to allow individuals to take notes or use other personal devices to view and capture images of their own PHI.
  - Proposed Rule would allow individuals to direct the exchange of PHI in an EHR among providers and health plans; which would require the provider or health plan to submit an individual's access request to another provider and to receive back the requested ePHI. Correspondingly, providers and health plans would be required to respond to these requests.
  - Permissible fee structure would be revised to limit fees for requests to direct electronic copy of records to a third party to reasonable cost-based fee limited to labor for making copies. Covered entities would be required to post estimated fee schedules on their websites.

Proposed Privacy Rule Revisions

Key provisions

- **Health Care Operations / Care Coordination and Case Management**
  - Definition of "health care operations" would be amended to clarify the scope of permitted uses and disclosures for individual-level care coordination and case management.
  - An exception to the minimum necessary rule would be created for individual-level care coordination and case management uses and disclosures, so that the minimum necessary rule would not apply to such coordination and case management uses and disclosures even if such activities were considered health care operations (instead of treatment activities).
  - Clarification that covered entities are expressly permitted to disclose PHI to social services agencies, community-based organizations, home and community-based service providers, and other similar third parties that provide health-related services, to facilitate coordination of care and case management for individuals.
- **Notice of Privacy Practices**
  - NPP would be required to include provisions regarding (1) how to access PHI; (2) how to file a HIPAA complaint; and (3) right to receive a copy of the NPP and to discuss its contents with a designated person.

EPSTEIN
BECKER
GREEN

42 C.F.R. Part 2

42 C.F.R. Part 2 Basics

- Part 2 Program
  - Federally assisted, which includes nonprofits, Medicare providers, and organizations that receive federal licensure, certification or registration (e.g., to dispense controlled substances).
  - Program:
    - A person (other than a general medical facility) that holds itself out as providing, and provides, SUD diagnosis, treatment or referral for treatment; or
    - An identified unit within a general medical facility that holds itself out as providing, and provides, SUD diagnosis, treatment, or referral for treatment; or
    - Medical personnel or staff in a general medical facility whose primary function is the provision of SUD diagnosis, treatment or referral for treatment and who are identified as such providers.
  - QSO –Analogous to a business associate.
  - Lawful Holder: Recipient of Part 2 records pursuant to a consent or a consent exception.

2024 Part 2 Final Rule Changes (effective 2/16/26)

Goal: Revise Part 2 to better align with HIPAA

1. One Time TPO Consent: Permits patients to provide a one-time TPO consent without expiration
   - Once prior consent is obtained**, HIPAA Covered Entities and Business Associates may use and disclose SUD records for TPO as permitted by HIPAA and re-disclose as permitted by HIPAA.**
2. Patient right to Accounting of Disclosures
3. Applies HIPAA Breach Notification Rule to Part 2
4. Applies HIPAA criminal and civil enforcement mechanisms to Part 2
5. Prohibits use or disclosure of Part 2 Records for civil, criminal, administrative or legislative proceedings against the patient.
6. Allows a Part 2 Program to disclose de-identified data to public health authorities
7. Changes to Part 2 NPPs

Key Takeaways

- Heightened enforcement risk
- Operational challenges to address multiple consents/authorizations
  - Limited Part 2 Consent
  - One-time TPO Consent
  - Consent for use or disclosure of Part 2 Records for civil, criminal, administrative or legislative proceedings against the patient.
- Hard decisions on whether to condition treatment on limited or general consent
- Challenges with Health IT
  - Locking down/segregating (which is no longer necessary in theory) Part 2 Records
  - Attaching consents to SUD records when disclosed

EPSTEIN
BECKER
GREEN

HIPAA RHI Rule Vacated

RHI Rule Vacated

- April 26, 2024, Final Rule *HIPAA Privacy Rule to Support Reproductive Health Care Privacy* published in response to Supreme Court decision in *Dobbs v. Jackson Women's Health Organization* and then-President Biden's Executive Order instructing HHS to "consider additional actions to improve privacy protections for sensitive reproductive health information…".
- Among other things, the Final Rule prohibited disclosure of lawful reproductive health information when requested under certain exceptions, including law enforcement exception. Required covered entities to obtain attestation from requestors of reproductive health information affirming lawful purpose of the request.
- June 18, 2025, in *Purl v. United States Department of Health and Human Services*, the U.S. District Court for the Northern District of Texas vacated the Final Rule finding the Final Rule:
  1. Contradicted the HIPAA statute which provides: "…nothing in [HIPAA] shall be construed to invalidate or limit the authority … established under any law providing for [various public health activities]…";
  2. Unlawfully redefines HIPAA statutory terms "public health" and "person"; and
  3. Was adopted without authority expressly delegated by Congress as the statute gave HHS authority to regulate "individually identifiable health information" but not "reproductive health information" specifically and thus: "…it confers no authority to distinguish between types of health information to accomplish *political* ends like protecting abortion…".

The Current Landscape

What Changed?

- Attestation requirements for disclosing reproductive health information (RHI) are no longer required.
- Enhanced prohibitions on disclosing RHI for investigations are removed.

What Stays the Same?

- Return to Status quo: The standard HIPAA Privacy Rule still applies to all PHI, including reproductive health.
- Applicable state laws regarding reproductive health privacy still apply.
- Part 2 substance use disorder NPP updates are still required by Feb. 16, 2026.

EPSTEIN
BECKER
GREEN

Medical Information of Minors

Ohio HB 162: My Child My Chart Act

- New RC 3798.05 which states (as currently drafted):

  …a health care provider shall ensure to the fullest extent permitted under the HIPAA privacy rule and Ohio law that the minor's parent or guardian has access in that system to the minor's health records. Additionally, a health care provider shall not require the minor's parent or guardian to obtain the minor's authorization before the parent or guardian may access in the electronic health records system records relating to care the minor received with parent or guardian consent.

- Additionally, RC 3798.05 would require:
  - Providers to information each minor’s parents annually (1) circumstances in which minor may consent to treatment without parental consent under Ohio law and (2) medical information regarding care consented to by minor without parent consent may not be disclosed to parents without minor’s authorization.
  - At “each minor’s annual well visit” provide the minor with opportunity to give general, ongoing authorization allowing parents access to medical information regarding treatment “that the minor patient may have consented to, or may consent to in the future, without parent or guardian consent”.

HIPAA Guidance

- December 3, 2025, OCR issued "Dear Colleagues" letter regarding "The HIPAA Privacy Rule and Parental Access to Minor Children's Medical Records".
- Key provisions of the Letter:
  - In most cases, a parent is the personal representative of an unemancipated minor child (hereinafter, "child") and can exercise the child's rights with respect to PHI, because the parent usually has the authority to make health care decisions about his or her child. Accordingly, the Privacy Rule generally gives the parent the right to access the child's medical records as the child's personal representative, unless one of the limited exceptions applies.
  - [*Exceptions include*] … When the child consents to health care and the consent of the parent is not required under state or other applicable law. In this situation, the parent is not the child's personal representative with respect to PHI related to ***that*** health care. (Emphasis in original.)
  - **Absent these limited exceptions, where a parent is the personal representative of his or her child, a covered entity (and, where applicable, its business associate acting on the covered entity's behalf) may not place additional limitations on a parent's access to the child's medical records beyond any existing limitations in applicable law.** (Emphasis in original.)

HIPAA Guidance

- Scenarios used in the Letter:

  Consider the following scenarios where, absent the existence of an applicable and specific exception, a parent cannot be denied access to his or her child's PHI:

  - A patient is 16 years old, consents to receive treatment for a sexually transmitted infection, and there is a state law that permits children who are 16 years or older to obtain such treatment without parental consent. A covered health care provider might, depending on the particular state law, deny the child's parent access to PHI related to that health care. However, the provider may not deny the parent, as the child's personal representative, access to the child's PHI that is unrelated to that particular health care.
  - A patient is 13 years old, and a state law requires parental consent for patients under 15 years old to receive health care in all cases. A covered health care provider cannot require authorization from that 13-year-old child before the provider will give the parent access to the child's PHI. The covered health care provider could not deny the parent access to that child's health care records by claiming that the 13-year-old child had not authorized parental access.

HIPAA Guidance

- Regarding EHRs and patient portals the Letter states:

  With respect to electronic access to PHI, covered entities should work with any business associates involved in facilitating such access (e.g., electronic health record or patient portal vendors) to ensure that parents who are their children's personal representatives have electronic access to their children's PHI to the full extent required by the Privacy Rule. This includes establishing electronic access configurations to allow parents access to their children's PHI in accordance with the Privacy Rule. For example, if the default configurations of electronic information systems that maintain a child's PHI result in the improper denial of a parent's right, as the child's personal representative, to timely access the information, the covered entity should modify, or work with their business associate (if applicable) to modify, the default configurations to allow such access as required by the Privacy Rule. A covered entity that denies such access may be in violation of the Privacy Rule.

Litigation & Enforcement

- The State of Texas recently initiated litigation against Epic alleging that Epic is “Failing to Provide Proxy Access in Violation of Texas Medical Records Privacy Act”:

  Parents and guardians have a fundamental right to direct their children's health care and must be given access to their children's medical records to exercise this right. … Without parental proxy access, a minor-aged child could pursue medical care that directly contravenes the rights of parents and guardians to choose the manner in which to raise their child. … Rather than respect the rights of parents and guardians in Texas, Epic, through false, misleading, and deceptive conduct, imposes the beliefs of its non-Texas-based customers, particularly those without parental proxy access guarantees, on healthcare providers here. Epic delivers Texas-based healthcare providers a software system that automatically limits parental proxy access upon a child turning 12 years old in violation of Texas Law.

- Announcement from Attorney General’s office:

  …Epic exploits its control over patient medical records, data it does not own, to automatically hide children’s medication lists, treatment notes, and provider messages from parents when their child turns a mere twelve years old. These deceptive practices undermine the fundamental right of parents to direct their children’s healthcare and clearly violate [Texas law].

  We will not allow woke corporations to undermine the sacred rights of parents to protect and oversee their kids’ medical well-being,…

Litigation & Enforcement

- Right of Access enforcement initiative continues.
- Director of the HHS Office of Civil Rights Paula Stannard:
  - Stated that OCR has "heard that certain large health care facilities or their [electronic health record] vendors were denying parents the right to access their minor children's medical [records]—it might be that they could access certain records until the child…reached age 13, and then the child had to authorize" access.
  - Announced that OCR was "initiating compliance reviews of a number of large health care providers to ensure that parents receive timely access to their children's health information."

EPSTEIN
BECKER
GREEN

Enforcement Trends for 2026

OCR's Top 2026 Enforcement Priorities

1. **Proactive Risk Management & Security Rule Enforcement:** Simple risk analysis is not enough. OCR is scrutinizing active risk mitigation. Stricter requirements include mandatory documentation of all security policies and procedures, along with implementing 2025 security rule updates that make many "addressable" items mandatory.
2. **Ransomware Readiness & Breach Response:** Investigations will focus heavily on whether entities had adequate, tested, and updated security measures to prevent ransomware, along with the ability to respond to breaches within required timelines.
3. **Digital Health and Tracking Technologies:** Continued focus on the use of tracking pixels (e.g., Google/Meta pixels) that disclose PHI without proper authorization.
4. **HIPAA Right of Access Initiative:** Continued enforcement on ensuring patients receive timely, reasonably priced access to their records, with a new emphasis on parental access to minor records.
5. **Vendor/Business Associate Oversight:** Active scrutiny of how organizations vet, manage, and monitor their vendors to ensure PHI is protected throughout the supply chain.
6. **Part 2 Substance Use Disorder Records:** As of Feb 16, 2026, enforcement focus includes compliance with 42 C.F.R. Part 2.

Compliance Recommendations

1. **Upgrade Technical Safeguards:** The distinction between "required" and "addressable" security specifications has essentially been eliminated. Your practice must implement the following:
   - **Encryption:** Ensure all ePHI is encrypted both in transit and at rest (including databases, file systems, and backups).
   - **Multi-Factor Authentication (MFA):** Require MFA for all system access, not just for remote logins.
   - **Secure Communications:** Do not use standard SMS for patient communications. Use HHS-approved encrypted patient portals or messaging platforms.
2. **Update NPP:** Covered entities and federally assisted treatment programs must ensure their NPPs include new, specific language regarding the handling of SUD records and patient rights.
3. **Streamline "Right of Access" Workflows:** While HIPAA requires a turnaround time of 30 days, OCR is strictly prioritizing a 15-day turnaround for patient record requests to improve interoperability.
4. **Tighten Vendor and Business Associate Oversight:** Perform due diligence on all vendors. Ensure you have signed and updated BAAs with all vendors handling your ePHI. Maintain a comprehensive inventory of all software, devices, and systems with access to patient data.
5. **Document and Assess Risk:** Conduct an updated, documented Security Risk Assessment and proactively mitigate all identified vulnerabilities.
6. **Staff Training:** Ensure all employees complete annual HIPAA and security awareness training.
7. **Document, document, document!!**

EPSTEIN
BECKER
GREEN

SECURE Data Act

Proposed Federal Data Privacy Framework

The **SECURE Data Act** (Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act, H.R. 8413) is a comprehensive federal privacy bill introduced in the U.S. House of Representatives to establish a national framework for protecting consumer personal data.

Applicable to businesses processing data for over 200,000 consumers with at least $25 million in annual gross revenue.

Key Consumer Rights

If enacted, the legislation would give consumers new enforceable rights regarding how their personal information is used

- **Data Control:** The right to access, correct, delete, and port personal data.
- **Opt-Out Privileges:** The ability to opt-out of targeted advertising, profiling, and the sale of personal information.
- **Sensitive Data:** Businesses would be required to obtain consent before processing highly sensitive data, such as precise geolocation data.

Business Obligations

The bill applies to businesses operating under FTC jurisdiction that meet specific data-processing thresholds. Covered organizations must do the following:

- **Data Minimization:** Collecting only the data strictly necessary for a given service.
- **Security & Transparency:** Maintaining strict data security standards and providing enhanced disclosures.

Key Details and Status

Legislative Status:

Introduced on April 22, 2026, by House Republicans. The bill is awaiting further consideration and committee action. It currently lacks bipartisan support, with no Democratic co-sponsors.

Federal Preemption:

- If passed, the Act would broadly preempt existing and future state-level privacy laws, which is a point of significant contention as it would override stronger state protections like California's CCPA/CPRA.
- The Act does not relieve or change obligations under other various federal privacy laws (e.g., COPPA, GLBA, HIPAA/HITECH, FCRA, FERPA, human-subject protections, etc.)

Enforcement:

Enforcement would fall to the Federal Trade Commission (FTC) and State Attorneys General, with no private right of action for consumers.

Right to Cure:

The Act includes a right to cure. The FTC or a State AG must provide written notice identifying the specific alleged violation and wait at least 45 days before initiating an action; curing within that period (and providing a written assurance) eliminates the violation.

EPSTEIN
BECKER
GREEN

CIRCIA Rules (Expected in 2026)

CIRCIA

- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
  - Enacted in 2022, requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA.
- Proposed Rule published April 2024
  - Extensive reporting obligations for entities in 16 critical infrastructure sectors including HealthCare and Public Health.
  - Covered entities required to report “substantial cyber incident” within 72 hours. “Substantial cyber incident” defined as causing any of the following:
    - Substantial loss of confidentiality, integrity, or availability
    - Serious impact on safety and resiliency of operational systems and processes
    - Disruption of ability to engage in business or industrial operations or deliver goods or services
    - Unauthorized access facilitated through or caused by a compromise of a provider or third party or a supply chain compromise
  - Covered entities also required to report a ransom payment in response to a ransomware attack within 24 hours.

CIRCIA

- Proposed Rule published April 2024 (cont'd)
  - Updates/supplemental reporting required "promptly" if "substantial new or different information becomes available" or if the covered entity makes a ransom payment after submitting a covered cyber incident report.
  - Covered entity required to preserve data relevant to the covered cyber incident or ransom payment.
- Notes for hospitals:
  - Most hospitals will be "covered entities" subject to CIRCIA.
  - Exception to reporting requirements include when entity "required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe" and provided that the Federal agency receiving such reports has an agreement in place to share such information with CISA. Unlikely to apply to hospitals.
  - "Substantial cyber incident" does **not** require that PHI be involved in the incident and is **not** dependent on whether the incident is a HIPAA breach.
  - 72-hour and 24-hour reporting requirements much shorter than HIPAA breach reporting.

EPSTEIN
BECKER
GREEN

AI Issues

Building Trust with AI Governance

Key Governance Steps

- Board commitment to AI Governance
- C-Suite leaders must understand and commit to AI Governance principles
- Appoint individuals to oversee the AI Governance program including data stewards
- Develop policies and protocols to oversee AI Governance program
- Establish review and approval process to identify and manage risk related to AI deployment by the organization

Principles of Data Stewardship

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality & Integrity
- Security
- Accountability and Auditing

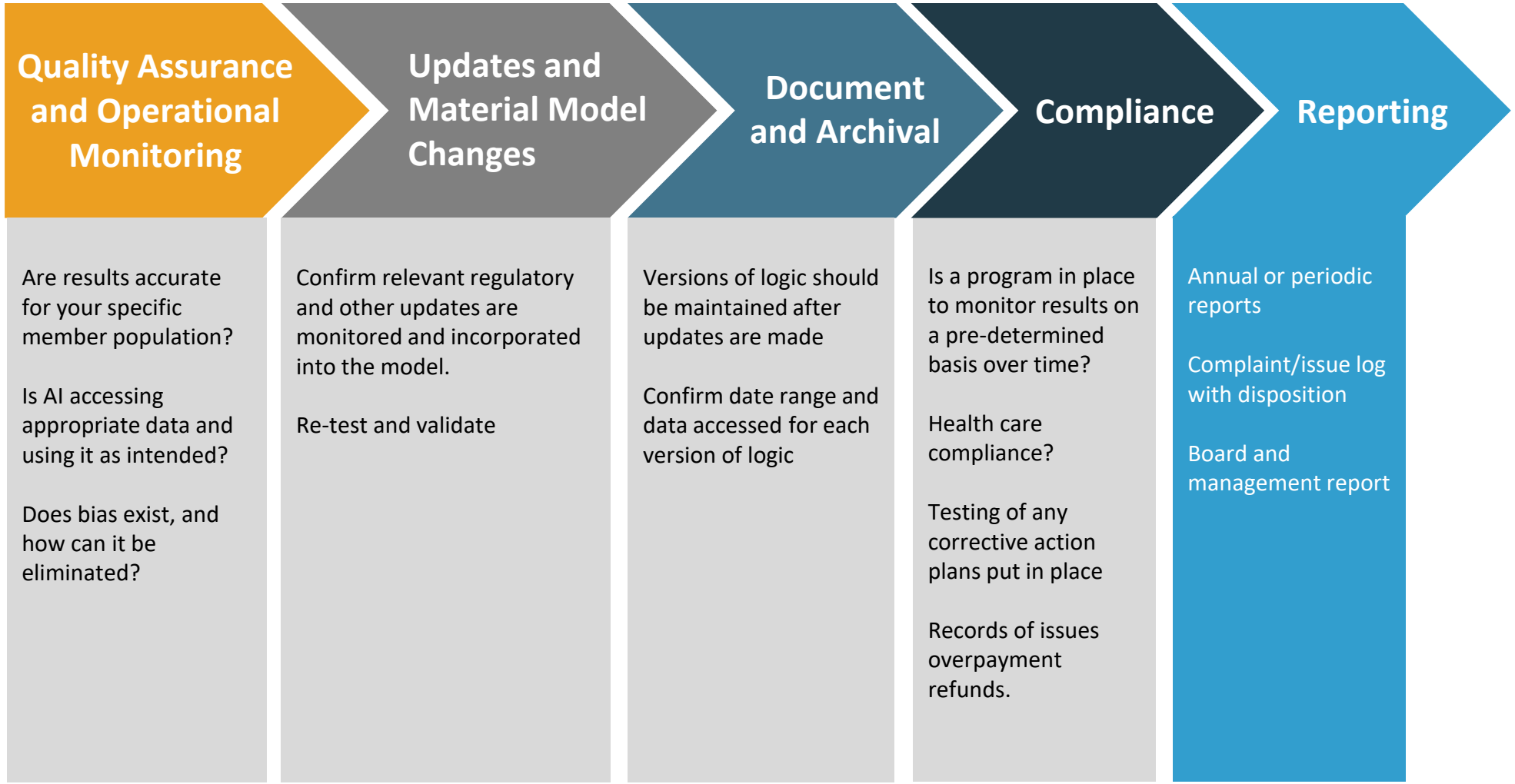
AI Due Diligence Prior to Deployment

- Who is responsible at the organization? AI Oversight Team?
- What is the scope of intended use?
- How to investigate and diligence?
  - Vendor (and software manufacturer where applicable)
  - Technology
  - Enforcement risks
- Engagement Hurdles and Challenges?
  - Legal Contract Review
  - Business Contract Review
  - Allocation of Risk, Liability and Indemnities
- What is the timeline and implementation plan?
- How to conduct pre-deployment testing and ensure validation prior to approval?

AI Contracting

- Establishing clarity on expectation of services
- Intellectual property protection
- Representations and Warranties
- Disclaimers of Warranties
- Allocation of Risk
  - Indemnification
  - Limitations on liability
- Insurance Requirements
- Changes in Law

Ongoing Activities After AI is Implemented



Adapting the 7 Elements of the OIG's Compliance Program Guidance for the Creation and Use of AI Tools

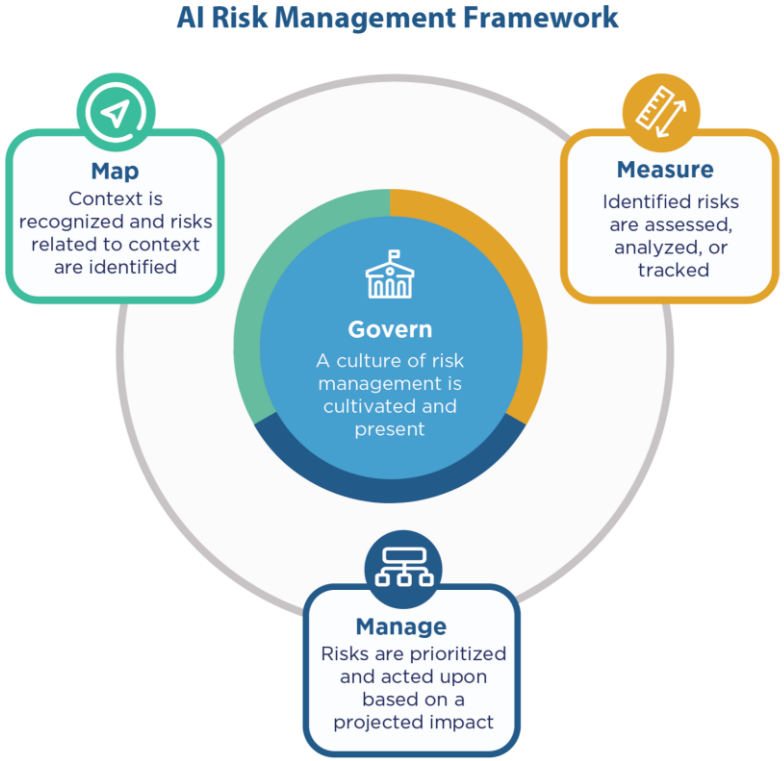
- Implement written policies, procedures and standards of conduct.
- Designate a compliance officer and compliance committee.
  - Designation of ownership of the AI risks.
  - Consider creating a committee charter.
- Conduct effective training and education.
- Develop effective lines of communication.
  - Reporting mechanism for concerns about AI tools.

- Conduct internal and external monitoring and auditing.
  - A risk assessment identifies high and moderate risk areas, which should be the focus on auditing and monitoring programs.
- Enforce standards through well-publicized disciplinary guidelines for failure to comply.
- Respond promptly to detected offenses and undertaking corrective action.

NIST Resources

- NIST-AI-100-1: AI Risk Management Framework (AI RMF)

Privacy and cybersecurity risk management considerations and approaches are applicable in the design, development, deployment, evaluation, and use of AI systems. Privacy and cybersecurity risks are also considered as part of broader enterprise risk management considerations, which may incorporate AI risks. As part of the effort to address AI trustworthiness characteristics such as "Secure and Resilient" and "Privacy-Enhanced," organizations may consider leveraging available standards and guidance that provide broad guidance to organizations to reduce security and privacy risks, such as, but not limited to, the NIST Cybersecurity Framework, the NIST Privacy Framework, the NIST Risk Management Framework, and the Secure Software Development Framework. These frameworks have some features in common with the AI RMF. Like most risk management approaches, they are outcome-based rather than prescriptive and are often structured around a Core set of functions, categories, and subcategories. While there are significant differences between these frameworks based on the domain addressed – and because AI risk management calls for addressing many other types of risks – frameworks like those mentioned above may inform security and privacy considerations in the **MAP**, **MEASURE**, and **MANAGE** functions of the AI RMF.



NIST Resources

- NIST-AI-600-1: AI Risk Management Framework: Generative AI Profile

GOVERN 1.1: Legal and regulatory requirements involving AI are understood, managed, and documented.		
Action ID	**Suggested Action**	**GAI Risks**
GV-1.1-001	Align GAI development and use with applicable laws and regulations, including those related to data privacy, copyright and intellectual property law.	Data Privacy; Harmful Bias and Homogenization; Intellectual Property
AI Actor Tasks: Governance and Oversight		

MAP 4.1: Approaches for mapping AI technology and legal risks of its components – including the use of third-party data or software – are in place, followed, and documented, as are risks of infringement of a third-party's intellectual property or other rights.		
Action ID	**Suggested Action**	**GAI Risks**
MP-4.1-001	Conduct periodic monitoring of AI-generated content for privacy risks; address any possible instances of PII or sensitive data exposure.	Data Privacy

EPSTEIN BECKER GREEN

Questions?

Presenters

Lisa Pierce Reisz
614-872-2440
LPierceReisz@ebglaw.com

Allen Killworth
614-872-2415
akillworth@ebglaw.com