Healthcare's Digital Frontier: Balancing AI Innovation and Privacy

Privacy+ Security Forum

Introduction

Donald DePass

Counsel, Privacy & Cybersecurity

Hogan Lovells

Charlotte Lewis Jones

AI, Product, and Privacy Strategic Legal Executive

Michelle Pritchard

Legal Specialist

Mayo Clinic

Agenda

- What is an AI system?
- AI in the Healthcare Industry
- Overview of Global AI Regulatory Landscape
- U.S. AI Regulation
- Practical Implications
- Risks & Challenges of AI in Health Care
- AI Governance Program
- Q&A

What is an AI system?

Privacy+ Security Forum

What is an ‘AI System’?

Privacy+ Security Forum

1. Designed to operate with elements of **autonomy**
2. Based on data and inputs (e.g., instructions), **infers** how to achieve a given set of objectives
3. Does so using **ML and/or logic** and knowledge based approaches
4. Produces **system-generated outputs** such as content, predictions, recommendations & decisions

Roles Related to AI Systems

Privacy+ Security Forum

There are several key roles that establish clear responsibilities and obligations throughout the AI lifecycle.

- Provider/Developer
- Deployer/User
- Importer
- Distributer
- Authorized Representative
- Operator

Provider vs. Deployer

‘Provider/Developer’ - develops an AI system or has an AI system developed with a view to placing it on the market or putting it into service under their

‘Deployer’ - uses an AI system under its authority in the course of its activities

AI in the Healthcare Industry

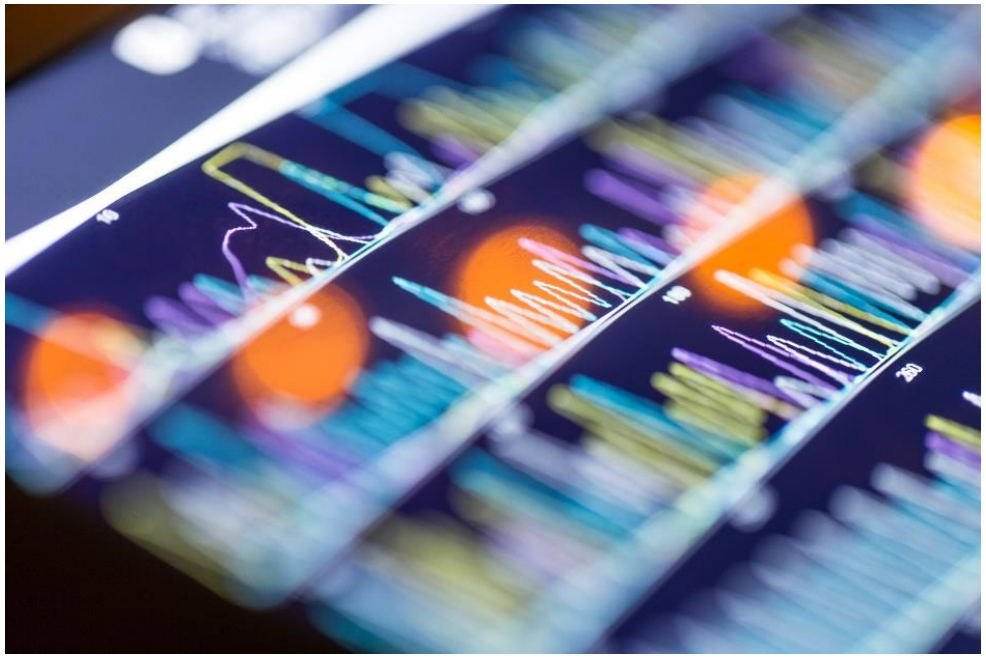
Privacy+ Security Forum

AI Tools

Potential to revolutionize operations, particularly in:

- Personalization
- Customer Service
- Predictive Analytics
- Price Optimization

Heightened Regulator Attention



How is AI Used in the Healthcare Industry?

Privacy+ Security Forum

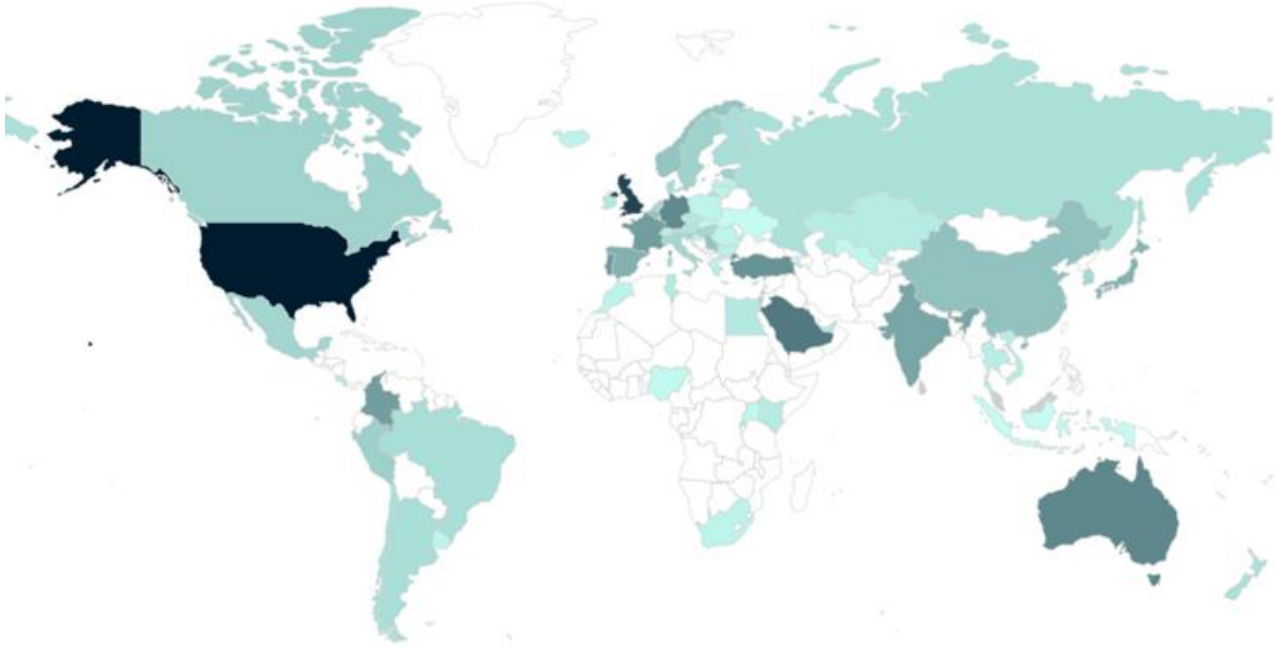
- Analyze medical imaging to detect and diagnose abnormalities
- Analyze medical data to recommend treatment options and create personalized treatment plans
- Interpret & standardize medical records
- Match patients to research and clinical trial opportunities
- Identify fraudulent or improper payments and authorizations; streamline operations
- Support drug & biologic application submissions
- Enhanced medical device design, engineering, and performance
- Technically safeguard sensitive information

Overview of Global AI Regulatory Landscape

Privacy+ Security Forum

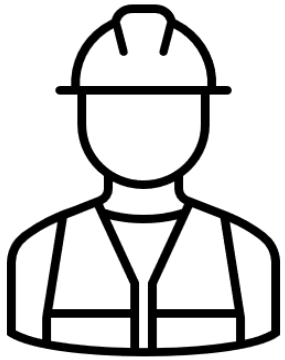
Global Public Policy & Legal Developments

- AI policy initiatives are global
- >70 countries have proposals, strategies, or frameworks
- Jurisdictions are quickly transitioning from ethical principles to regulatory obligations
- Data protection authorities are actively engaging



Visualization of countries with AI initiatives, colored by initiative count
Source: OECD.AI (2021), powered by EC/OECD (2021), database of national AI policies, accessed on 10/01/2024 https://oecd.ai

Focus of Proposed and Existing AI Regulations

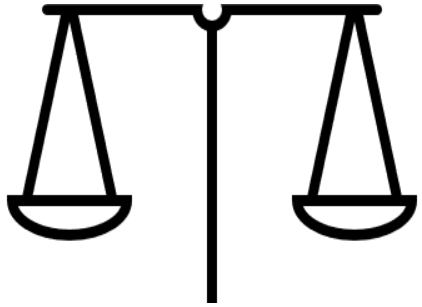


General harms

Reflect growing consensus on the need to address ethical, privacy, and safety concerns associated with AI.

Sectoral

Seek to address the unique challenges and risks within different industries.



Risk-based

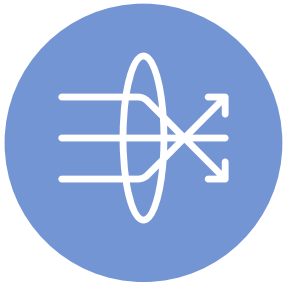
Tailor rules and requirements to the level of risk posed by different AI applications.

Categories of Focus of AI Regulations

Privacy+ Security Forum

Algorithmic Bias Fairness

Possibility of inherent bias causing discrimination



Automated Decision-Making

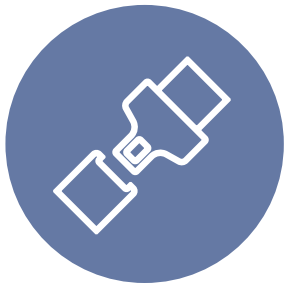
Overreliance on fully automated decisions without appropriate human oversight

Privacy

Risks associated with use of personal data for training, inputs, & outputs

Safety

Unintended results & outputs create risks of harm

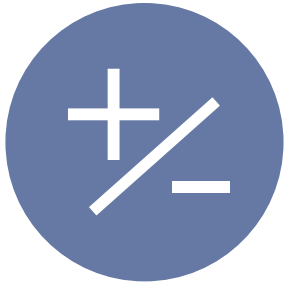


Transparency Explainability

Understanding of AI uses & decisions made by AI

Accuracy Performance

Potential for inaccuracies



United States AI Regulation

Privacy+ Security Forum

US Framework

- No comprehensive AI law at the federal level
- Patchwork of federal and state laws and guidelines
- Often sector specific
- Resulting in the lack of a uniform approach

Standards/Guidelines

- White House Principles/Executive Order
- Agency guidance
- FAVES
- NIST

Existing Federal Laws

- FTC Act
- HIPAA
- HTI-1
- Part 2 Regs
- GINA
- Congressional bills introduced

State Laws

- CO AI Act
- CA AI bills
- Consumer privacy laws
- Consumer protection laws
- Health privacy laws

Federal Developments

Privacy+ Security Forum

Select Federal Policies and Guidelines

Privacy+ Security Forum

White House	**Blueprint for an AI Bill of Rights & WH EO on AI** • Blueprint: est. 5 principles to guide design & use of covered systems • EO on AI: est. comprehensive guidelines for responsible development, deployment, and use of AI • FAVES: **F**air, **A**ppropriate, **V**alid, **E**ffective, **S**afe for health care outcomes
National Institute of Standards and Technology	**AI Risk Management Framework and related documentation** • Guidelines to help orgs improve the ability to incorporate trustworthiness into design, development, use, and evaluation of AI systems
Federal Trade Commission	**Multiple guidance documents** • Concerns about AI usage and discrimination; recommendations promoting testing, transparency, and accountability; settlement of AI-related claims
U.S. Dept. of Health & Human Services	**Engagement by multiple agencies - for example:** • FDA: AI and med products guidance; cleared, authorized, approved AI-enabled devices • ONC: HTI-1 rule to increase algorithm transparency for predictive AI used in EHRs • CMS: Exploring whether algorithms used by health plans & providers introduce bias/impede access to care

Key US Federal Health Law Considerations

Health Insurance Portability and Accountability Act (HIPAA)

- Permissible use of PHI
- Covered entity versus business associate
- Health care operations versus research
- De-identified data (safe harbor versus statistician method)

Office of the National Coordinator for Health Information Technology (ONC) Rule

- Predictive decision support interventions integrated into certified health IT
- Nutrition label on risk management (design, development, training, evaluation of predictive DSIs) for healthcare providers (HCPs) to understand limits or biases and confirm testing/validation
- Describe data governance, how data acquired, managed and used
- Evaluate and mitigate risks regarding accuracy, bias and safety

Other US Federal Law Considerations

Section 5 of the FTC Act

- Use of sensitive data without express consent
- Misleading representations, lack of transparency
- Tested/validated/bias/assessment of risks
- Training and governance
- Disgorgement of algorithms

FTC Guidance on AI Tools

- Deceptive trade practices
  - Misleading consumers about **the nature of AI tools** or **their outputs**
  - Misleading consumers about **what AI-based products can do**
    - Tools to identify AI-generated content
    - Representing outputs as human-generated
  - Misleading consumers about AI tools' **collection** and **deletion** of data

FTC Guidance on AI Tools

- Unfair trade practices
  - A practice or act is “unfair” under Section 5 if it causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.
  - The use of AI or other automated decision-making systems can be unfair if they make **biased, discriminatory, or incorrect** decisions about individuals that could have been avoided (see *Rite Aid*)

FTC Guidance on AI Tools: Best Practices

Privacy+ Security Forum

- Carefully review claims about AI tools, and the circumstances around their use, to make sure that consumers are not deceived, and be especially transparent about the use of sensitive data, including when training algorithms
- Don’t give consumers the wrong impression
- Make sure that AI models are validated and revalidated to work as intended, and do not illegally discriminate
  - How representative is your data set?
  - Does your model account for biases? Make sure inputs are not proxies for protected classes
  - How accurate are your predictions?
  - Does your reliance on big data raise ethical or fairness concerns?

State Law Developments

Privacy+ Security Forum

U.S. State Law Landscape

- State laws vary but can impose stricter requirements
  - Legacy consumer protection & health privacy laws (e.g., sensitive conditions)
  - Some more targeted laws appearing, particularly for use of AI in higher risk settings or that may impact consumer safety
- Colorado AI Act
- California developments
- State privacy laws on automated decision-making and profiling
- State consumer health privacy laws
- State consumer protection law enforcement
- Intersections and exemptions

Colorado AI Act

- Effective 2/1/26, but likely to change
- High risk AI systems (consequential decision, essential services, material impact)
- Developers/deployers
- Use reasonable care to protect consumers from known or reasonably foreseeable risks of algorithmic discrimination
- Rebuttable presumption if compliance with law:
  - Disclosures, risk management policy/program regularly reviewed and updated, impact assessments

Privacy Laws on Automated Decision Making and Profiling

- Growing trend of state privacy laws that restrict automated decision making and profiling
  - Most states with comprehensive privacy laws include an opt-out right for profiling used for consequential decisions, although there's some variation
  - Colorado has specific requirements for data protection assessments and notices for consumers (e.g., describing the decision made, the training data/logic used, the degree of human involvement, and any fairness/disparate impact assessments)
  - California is considering new rules for automated decision-making opt-outs and impact assessments
  - California's authority is broad and could go beyond tools used for consequential decisions

Consumer Health Data Privacy Laws

- **Washington My Health, My Data Act (MHMD), Nevada Consumer Health Data Privacy Law (SB 370), Connecticut Connecticut Data Privacy Act Amendment (SB 3)**

- Requirements vary by law and may include:
  - consent for collection, sharing, and selling of consumer health data
  - giving consumers various rights related to their health data (e.g., access, delete)
  - provision of a consumer health data privacy policy

Intersections & Exemptions

- HIPAA entity- and data-level carve-outs
- Not for profit carve-outs
- Research data carve-outs

California Developments – AB 3030

- Among the many AI bills introduced in 2024, health-specific AB 3030 was signed into law
- Requires that certain HCPs that use generative AI to generate patient communications pertaining to patient clinical information to ensure that those communications include:
  - A disclaimer that indicates to the patient that a communication was generated by AI
  - Clear instructions describing how a patient may contact a human health care provider, employee of the health facility, clinic, physicians office, or office of a group provider, or other appropriate person.
- Exception: Above requirements inapplicable if communication is generated by gen AI but read and reviewed by a human licensed or certified HCP

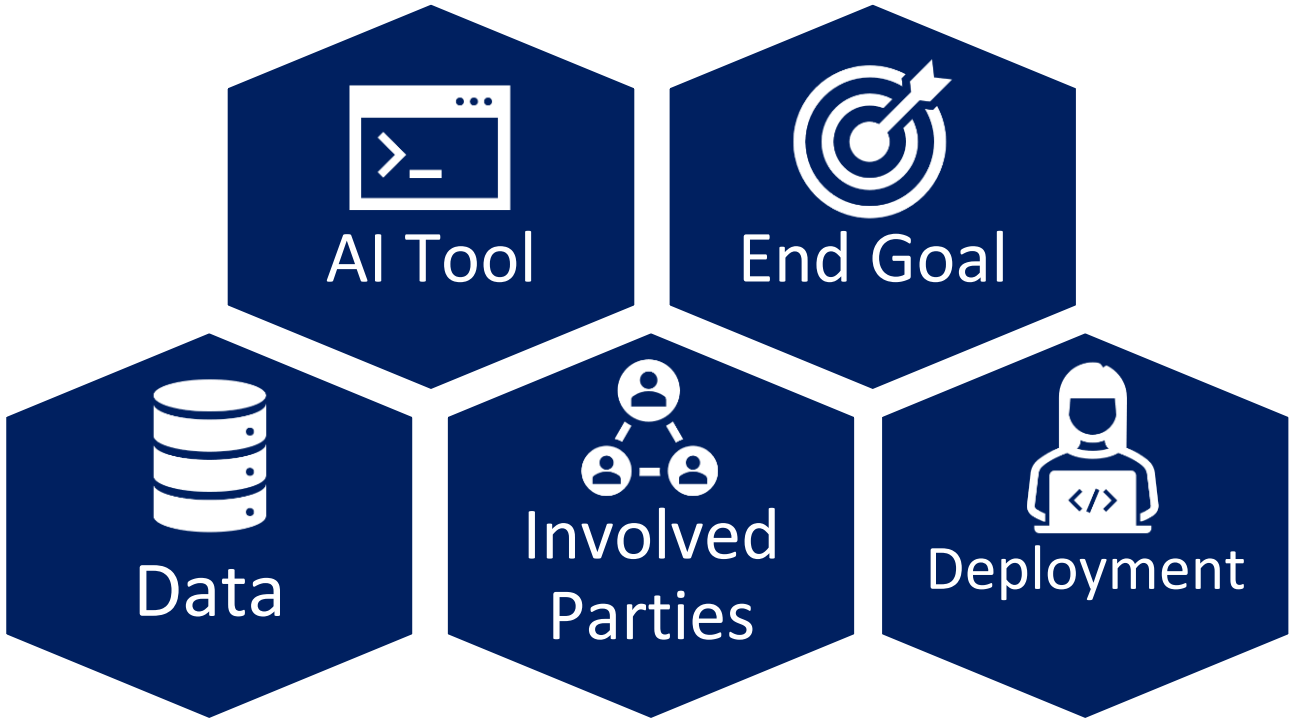
Texas AG Enforcement – Pieces Technologies

- In Sept. 2024, TX AG announced settlement with gen AI health tech company, Pieces
- Alleged **B2B communications** about AI-powered services violated TX consumer protection law
- Settlement with 5 year term:
  - Marketing statements regarding metrics related to gen AI outputs must contain certain disclosures
  - Prohibition on making false, misleading, or unsubstantiated representations
  - Customer documentation disclosing known / reasonably knowable harmful uses or misuses of products

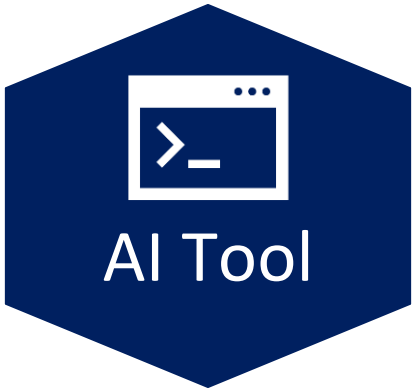
Practical Implications: Healthcare Providers as Developers

Privacy+ Security Forum

Healthcare Providers as Developers



Healthcare Providers as Developers



- Intended use
- Code
- Current stage of development

Healthcare Providers as Developers

- Commercialization/research
- Publication/public discourse
- Billing

Healthcare Providers as Developers

- Training and validation data make-up
- Data collection
- Volume
- Identifiability

Healthcare Providers as Developers

- Access to and use of data
- Third-party software dependencies
- Allocation of responsibility

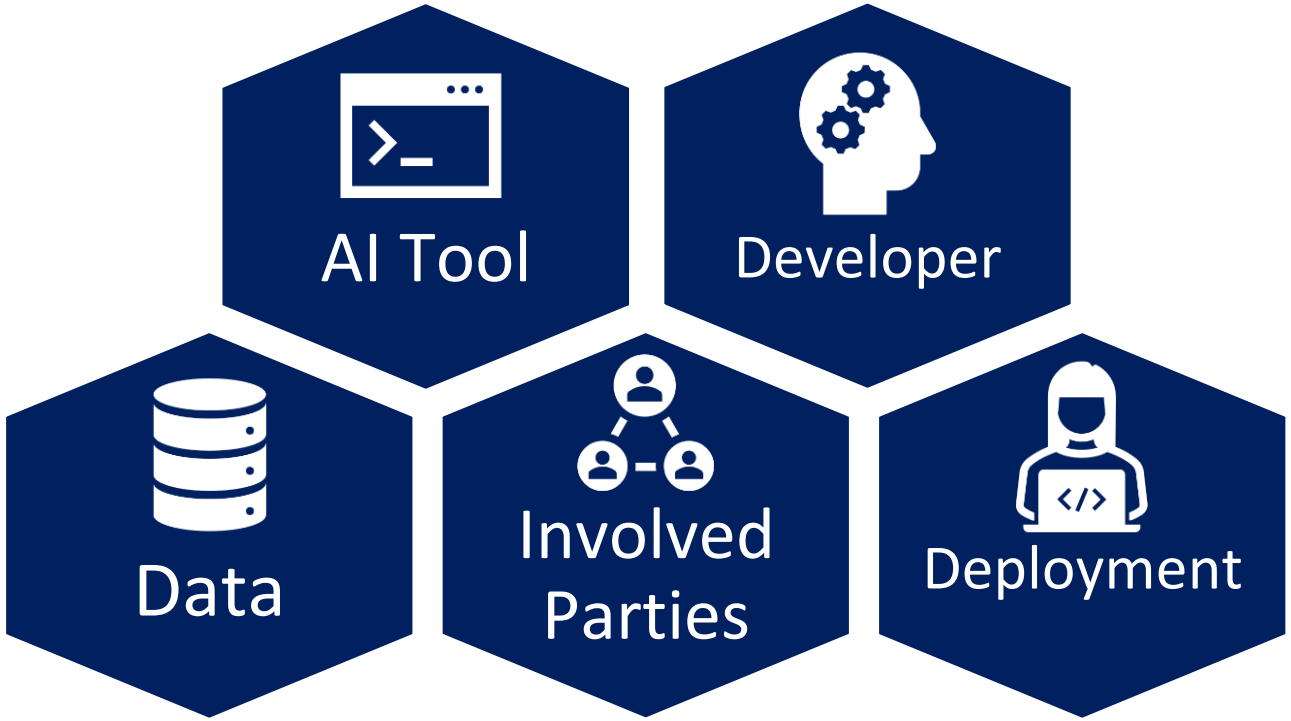
Healthcare Providers as Developers

- Intended users
- Intended markets (i.e., countries, states)
- Research use, clinical practice, direct to consumer

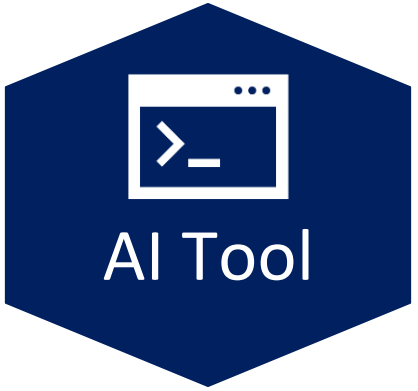
Practical Implications: Healthcare Providers as Deployers

Privacy+ Security Forum

Healthcare Providers as Deployers



Healthcare Providers as Deployers



- Intended use
- Type of model

Healthcare Providers as Deployers

- Third party developer or internally developed
- Agreement terms
- Developer support

Healthcare Providers as Deployers

- Data inputs (data elements, data subjects, data collection)
- Security controls
- Data access
- Consent
- Integration into HCP systems

Healthcare Providers as Deployers

- Access to and use of data
- Third-party software dependencies

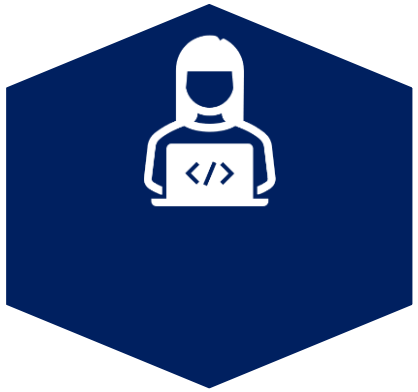
Healthcare Providers as Deployers

- End user(s)
- Individuals affected by the tool's use
- Location of deployment (geographical and departmental)
- Research use, clinical practice, direct to consumer
- User training
- User labeling
- Notices to end user(s) and affected individuals

Practical Implications: Service Providers to Healthcare Providers

Privacy+ Security Forum

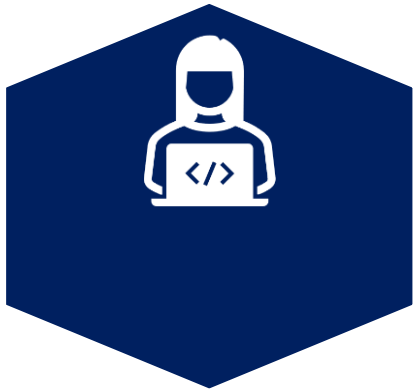
Service Providers to Healthcare Providers



HIPAA Compliance

- When acting as a business associate, confirm AI systems and processes enable compliance with HIPAA Privacy, Security, and Breach Notification Rules
- These rules require safeguards for the use and disclosure of PHI and secure transmission of health data
- Is your subcontractor's use of PHI within AI systems consistent with HIPAA and other relevant laws?

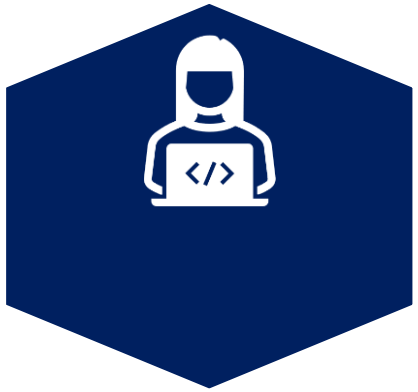
Service Providers to Healthcare Providers



Commercial Obligations

- You may need to sign a Business Associate Agreement (BAA) with each healthcare provider and the relevant subcontractors
- These agreements outline your permitted use and disclosure as well as responsibilities when handling PHI
- Do your AI subprocessor agreements (and subcontractor BAAs) align with your customer BAA promises?

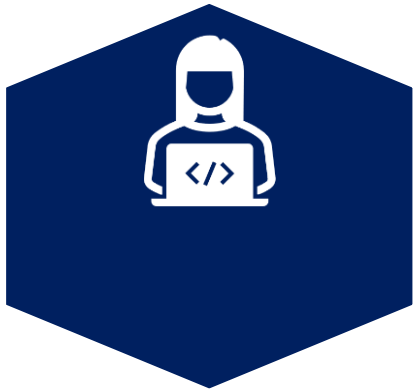
Service Providers to Healthcare Providers



Data Security and Incident Response

- Healthcare data is highly sensitive; leading practices to protect its use within AI systems include:
  - implementing robust data protection measures both in transit and at rest (e.g., encryption, access controls)
  - using encryption methods that meet or exceed regulatory standards
  - implementing data incident and breach response plans
- Do your security measures match any new risks created by the use of AI systems (e.g., specific vulnerabilities, abuse patterns)?

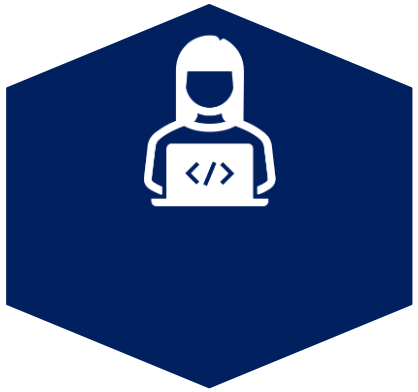
Service Providers to Healthcare Providers



Disclosing the Use of AI Systems

- If the use of your technology is not clear, why might you “announce yourself” and how do you do it?
- If you are “behind” the healthcare provider, whose job is it to announce that an AI system is present? How do you avoid an “eavesdropping” claim?

Service Providers to Healthcare Providers



Patient Consent to the Use of AI Systems

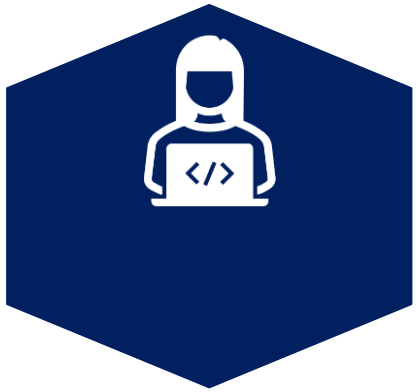
- Patient consent/authorization may be required for certain purposes (e.g., research)
- Such consent generally must be clear and conspicuous and contain certain content; depending on the service or product, such consent can be challenging to obtain
- How can patients be truly informed of something as complex as AI in a short period?

Service Providers to Healthcare Providers

Third Party Risk Management

- The allocation of risk between you and your AI subprocessors should be documented, specifically re the provider role within different business models (e.g., referring, white labeling, integrating)
- What diligence do you conduct for AI subprocessors under different business models? Where is there more risk and responsibility for you?
- For service providers that are “deemed” developers (not actual developers), are your obligations in line with your amount of control?

Service Providers to Healthcare Providers



Third Party Risk Management

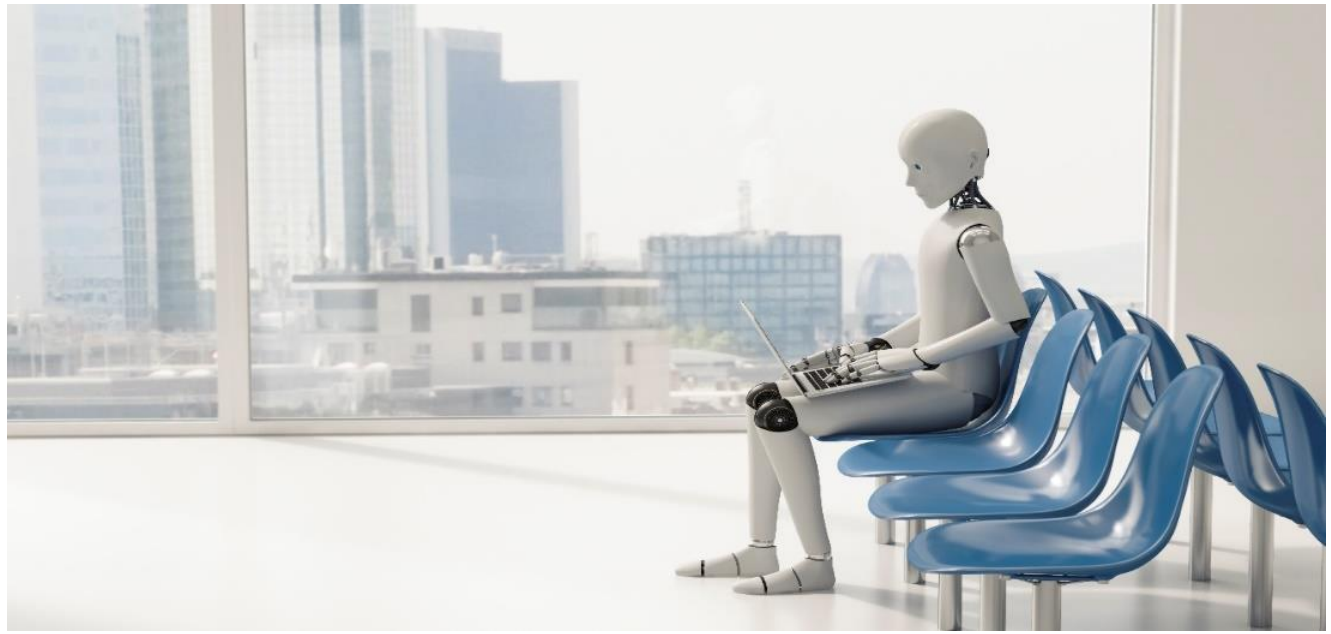
- How do you manage risk and customer expectations against which you cannot directly mitigate?
- How do you communicate details about AI systems you did not develop?
- What measures do you have in place to ensure your AI subprocessors have tested for and mitigated bias outcomes?

Risks & Challenges

Privacy+ Security Forum

Unintended Results: Harms

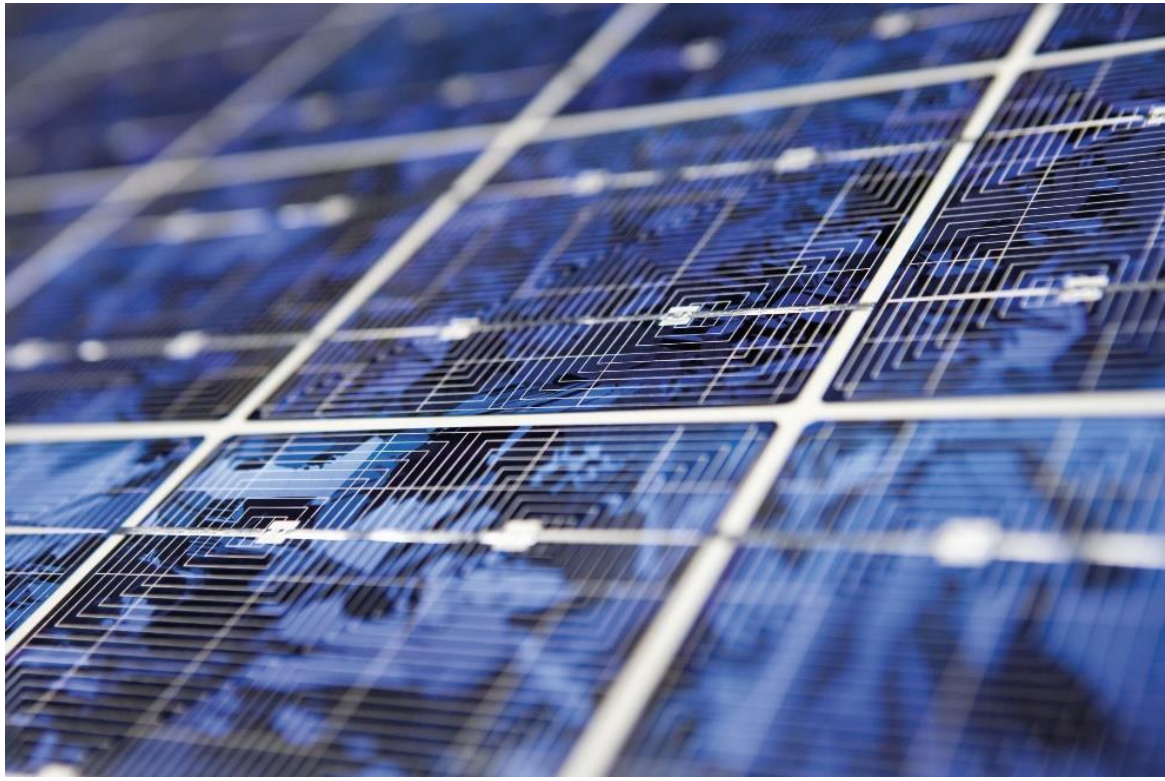
- Algorithmic bias
- Unequal access
- Diagnostic errors / inaccuracies
- Wrongful denials of coverage
- Privacy breaches
- Patient distrust
- Overreliance on technology



"Without appropriate testing, risk mitigations and human oversight, AI-enabled tools used for clinical decisions can make errors that are costly at best - and dangerous at worst." – *Biden Administration fact sheet on AI in healthcare.*

Consequences of Noncompliance

- Violations of applicable laws
- Regulatory investigations
- Technical and operational restrictions
- Prohibition of sale/use of AI system
- Required corrective actions
- Algorithmic disgorgement
- Reputation damage
- Financial impact



Building an AI Governance Program

Privacy+ Security Forum

10-Step AI governance checklist

Privacy+ Security Forum

1. Identify **scope** of AI system developed and used
2. Establish responsibility for **AI oversight**
3. Introduce **AI/algorithmic risk management** framework
4. **Assess compliance** of existing AI systems and **mitigate risks**
5. Review **use of personal data** in AI lifecycle
6. Implement **policies** and **procedures**
7. Introduce **human oversight** into algorithmic decisions
8. Review existing approach to **vendor management**
9. Implement **testing and monitoring** procedures
10. **Provide training** to product development teams

Questions?

Privacy+ Security Forum

Donald DePass
donald.depass@hoganlovells.com

Charlotte Lewis Jones
charlotte.lewis@aya.yale.edu

Michelle Pritchard
pritchard.michelle@mayo.edu

Thank You

Privacy+ Security Forum