RIMÔN

The data protection implications of AI and similar technologies on healthcare in the EU and U.S.

Privacy & Security Forum – 25 October 2024

Peter McLaughlin
Partner – Data Privacy

The Executive Order and Healthcare

- The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO), signed by President Biden on October 30, 2023

- Immediate Actions: HHS is directed to establish an AI Safety Program by October 2024, partnering with patient safety organizations to track and address clinical errors from AI in health care.
  - FDA; ONC; OCR

- HHS Policy Activities: The Department of Health and Human Services (HHS) has initiated specific policies to oversee AI-enabled health technology, including FDA guidance on AI-based software as medical devices.

- AI Safety Program Goals: The program will develop a framework for capturing and analyzing incidents caused by AI, generate guidelines to avoid harm, and disseminate these guidelines to stakeholders.

- Quality and Non-Discrimination Strategies: HHS will develop strategies for quality assessment, compliance with non-discrimination laws, and AI regulation in drug development.

The FDA and Software in *or* as a Medical Device

- FDA Regulation Criteria: AI- or ML-enabled software that meets the statutory definition of a "medical device" is subject to FDA regulation under the Food, Drug, & Cosmetic Act.

- Definition of Medical Device: A medical device includes any instrument, apparatus, implement, machine, implant, in vitro reagent, or similar article intended for diagnosis, treatment, or prevention of disease.

- Software as a Medical Device (SaMD): SaMD refers to software used for one or more medical purposes without being part of a hardware device.

- Standalone Functionality: Most AI- or ML-enabled software can operate independently as SaMD, unlike software that is an integral part of medical device hardware.

- Intended Use: AI- or ML-enabled SaMD products have a standalone intended use, while AI- or ML-enabled software in medical devices typically does not.

The FDA and Software as a Medical Device – Scope

- Establishing Intended Use: The FDA starts determining if AI or ML software is a medical device by defining its intended use based on the developer’s claims, including labeling, materials, promotion, and advertising.

- Indications for Use: A short statement called "indications for use" describes what the AI or ML does, who will use it, the context of use, and any limitations, forming the basis for regulatory strategies and marketing claims.

- Risk-Based Regulation: The FDA regulates medical devices based on risk, with higher-risk AI or ML products requiring more stringent oversight to ensure safety.

- Clinical Risk Analysis: Regulatory analysis often involves evaluating clinical risks, requiring the input of physicians to determine the necessity and extent of FDA oversight.

- Physician Perspective: Physicians play a crucial role in interpreting clinical risks and understanding regulations and exemptions from FDA oversight.

The FDA and Software as a Medical Device – Exemptions

Exemptions do apply:

- Certain Software Categories Are Exempted: Understanding exempted software categories is essential for developers and physicians to navigate FDA regulations and ensure compliance.

- Enforcement Discretion Category: The FDA may choose not to enforce compliance for certain low-risk AI or ML functions, categorizing them under "enforcement discretion."

- Research Software Regulation: Software intended for research that meets the definition of a medical device is regulated under different rules, such as the investigational device exemptions.

- ONC (HIT) regulates certain categories of operational software, such as Electronic Health/Medical Records

The FDA and the QMS Requirements

- Quality Management System (QMS) Requirement: AI- or ML-enabled software products often need a documented QMS before commercial release.

- Components of a QMS: An FDA-compliant QMS includes policies, procedures, and documentation aligning with good manufacturing practices and company operations.

  - Design Controls: QMS design controls encompass design planning, design inputs (user needs and risk controls), design outputs (user materials), verification, validation, and processes for clinical deployment.

  - Verification and Validation: Verification ensures the product functions as intended, while validation ensures it works in its intended setting.

  - Compliance Checks: FDA investigators check for document and record compliance, effective management, resource allocation, and required administrative controls.

  - Administrative Controls: These include audit programs, complaint handling, corrective actions, and mandatory reporting of certain events to the FDA.

ONC and Electronic Health Records, DSIs

- “Health Data, Technology, and Interoperability,” (HTI-1) final rule, which includes first-of-its-kind federal requirements for artificial intelligence (AI) and machine learning (ML)-based predictive software in health care.

- This rule impacts a wide range of technologies—referred to as predictive decision support interventions (predictive DSIs)—and directly applies to health information technology, including electronic health records (EHRs), which ONC certifies as having specific technical capabilities. Certified EHRs, which more than 96 percent of hospitals and 78 percent of office-based clinicians use nationwide, are the foundation of digital health care in the US.

  - Transparency in AI Development
  - Information Access for Users
  - Risk Management Practices
  - Technical Capability Requirement
  - Compliance with FDA Guidelines

OCR (Office of Civil Rights) and Non-Discrimination

- OCR is largely responsible for the protection of … civil rights

- Non-Discrimination
  - Section 1557 of the Affordable Care Act (“Section 1557”), which prohibits discrimination on the basis of race, color, national origin, age, disability, or sex (including pregnancy, sexual orientation, gender identity, and sex characteristics), in covered health programs.

  - OCR has issued a ”final rule” to consider how the increasing use of AI, among other tools, in health programs and activities could lead to discrimination and applies the nondiscrimination principles under Section 1557 to the use of “patient care decision support tools” in clinical care (a new defined term covering what we’ve known as clinical decision support tools/systems).
    - Reasonable efforts to ensure non-discrimination
    - Covered entities may not be aware of the datasets used by developers to train “patient care decision support tools,” and does not require that the covered entity obtain such data sets as part of their obligations

- HIPAA’s Privacy, Security, Breach Notice rules
  - Data security, integrity, availability

THANK YOU

Peter McLaughlin
peter.mclaughlin@rimonlaw.com
+1.617.480.1545