Overview of AI/ML as part of the FDA digital health arena

Cindy Jacobs, RN, JD

Affiliate Faculty, UW School of Law

Regulatory Analyst/Consultant, UW ITHS Technology Development Center

Digital Health Definitions—FDA

- Software as a Medical Device: Software intended for one or more medical uses that may run on different operating systems or in virtual environments. Software run on a hardware medical device is a SaMD when not part of the intended use of the hardware medical device. This can include standalone software that is intended to run on general-purpose computers or mobile platforms (e.g., smartphone, tablet). **Software is not SaMD if it drives or controls the hardware medical device**.

Digital Health Definitions—FDA

- Artificial Intelligence: A device or product that can imitate intelligent behavior or mimics human learning and reasoning. Artificial intelligence includes machine learning, neural networks, and natural language processing. Some terms used to describe artificial intelligence include computer-aided detection/diagnosis, statistical learning, deep learning, or smart algorithms.

Digital Health Definitions—FDA

- One rapidly growing area of Artificial Intelligence is machine learning. Machine learning is used to design an algorithm or model without explicit programming but through the use of automated training with data (e.g., a regression function or deep learning network). Devices that include Adaptive Algorithms, i.e., algorithms that continue to learn and evolve in time, are also another area of Artificial Intelligence.
  - FDA has a specific list of [cleared] Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices—total of 699 as of October 5, 2022 update.
- Interoperability: A device or product that can exchange and use information through an electronic interface with another medical/non-medical product, system, or device.

Digital Health Definitions—FDA

SPS ("What") and ACP ("How")

SaMD Pre-Specifications (SPS): A SaMD manufacturer's anticipated modifications to "performance" or "inputs," or changes related to the "intended use" of AI/ML-based SaMD. These are the types of changes the manufacturer plans to achieve when the SaMD is in use. The SPS draws a "region of potential changes" around the initial specifications and labeling of the original device. This is "what" the manufacturer intends the algorithm to become as it learns.

Algorithm Change Protocol (ACP): Specific methods that a manufacturer has in place to achieve and appropriately control the risks of the anticipated types of modifications delineated in the SPS. The ACP is a step-by-step delineation of the data and procedures to be followed so that the modification achieves its goals, and the device remains safe and effective after the modification.

Digital Health Definitions—FDA

- Novel Digital Health: A device or product that includes new, unfamiliar, or unseen digital health technology never submitted, cleared, or approved by FDA. The technology could potentially be a de Novo, have a new intended use, or have different technological characteristics. This also includes digital health technology or topic areas that have no agreed upon or established definition by industry or FDA.
- Examples of novel digital health technologies include but are not limited to:
  - Virtual Reality
  - Gaming
  - Medical Body Area Network (MBAN) wearable or implanted wireless devices

Digital Health Definitions—FDA

- RWD (real world data): data relating to patient health status and/or the delivery of health care routinely collected from a variety of sources.
- RWE (real world evidence): clinical evidence regarding the usage and potential benefits or risks of a medical product derived from analysis of RWD.

Digital Health Definitions—FDA

- Other assorted definitions
  - Advanced Analytics
  - Cloud
  - Wireless
  - Cybersecurity
  - Medical Device Data System
  - Mobile Medical App

Privacy/security issues r/t digital health devices

- Is FDA's jurisdiction related to privacy and security the result of magical thinking?
- FDA has no express authority under HIPAA statutes or regulations
- FDA frames this issue as a device safety issue, over which it does have authority/jurisdiction
  - "Patient harm is defined as physical injury or damage to the health of patients, including death. Cybersecurity exploits (e.g., loss of authenticity, availability, integrity, or confidentiality) of a device may pose a risk to health and may result in patient harm."

Privacy/security issues r/t digital health devices

- Device cybersecurity requires a multi-agency approach
  - FDA
  - NIST (National Institute of Standards and Technology)
  - Department of Homeland Security, Science and Technology
  - OCR (Enforcement—also enforces HIPAA)
  - FDA also works with other stakeholder organizations

FDA Cybersecurity Materials

- In collaboration with MITRE (a company "established to advance national security in new ways and serve the public interest as an independent adviser"), the FDA developed the ***Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook***,* a resource to help health care organizations prepare for cybersecurity incidents. The playbook focuses on preparedness and response for medical device cybersecurity issues that impact device functions.
- The Playbook was revised as of November 15, 2022
  - **Emphasizing the need to have a diverse team participating in cybersecurity preparedness and response exercises – including clinicians, health care technology management professionals, IT, emergency response, and risk management and facilities staff.**

*https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response

FDA Cybersecurity Materials

- Highlighting considerations for widespread impacts and extended downtimes during cybersecurity incidents which benefit from the use of regional response models and partners.
- Adding a resource appendix making it easier to find tools, references, and other resources to help health care organizations prepare for and respond to medical device cybersecurity incidents (including ransomware).

- A Playbook Quick Start Companion Guide is also available. The guide is a shorter version of the playbook that discusses preparedness and response activities health care organizations might want to start with as they are developing their medical device incident response program.

FDA Cybersecurity Materials

- October 7, 2022: FDA released a new video, "Tips for Clinicians - Keeping Your Patients' Connected Medical Devices Safe" (https://youtu.be/oxLbTPdtsLI) to help clinicians discuss cybersecurity of connected medical devices with patients. These tips focus on communicating with patients and aim to increase clinician comfort in approaching this topic.
- Other available materials at FDA digital health website pages*
  - Cybersecurity News and Updates
  - Mitigating Cybersecurity Risks
  - Cybersecurity Reports and White Papers

*https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

FDA Cybersecurity Materials

- Cybersecurity Safety Communications and Other Alerts
- Reporting Cybersecurity Issues
- MOUs on Cybersecurity in Medical Devices
- Workshops and Webinars on Cybersecurity
- Other Collaborations on Cybersecurity
- FDA Cybersecurity New Releases

Device Cybersecurity Guidance (Draft)

- ***Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions***
- Updated 4/8/2022
- This draft guidance replaces the 2018 draft version *(which had a different title)* and is intended to further emphasize the importance of ensuring that devices are designed securely, enabling emerging cybersecurity risks to be mitigated throughout the Total Product Life Cycle, and to outline the FDA's recommendations more clearly for premarket submission content to address cybersecurity concerns.

Device Cybersecurity Guidance (Draft)

- The need for effective cybersecurity to ensure medical device functionality and safety has become more important with the increasing use of wireless, Internet-and-network- connected devices, portable media (e.g. USB or CD), and the frequent electronic exchange of medical device-related health information. In addition, cybersecurity threats to the healthcare sector have become more frequent, more severe, and more clinically impactful.
- Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the US and globally. Such cyberattacks and exploits can delay diagnoses and/or treatment and may lead to patient harm.

Device Cybersecurity Guidance (Draft)

- This guidance is intended to provide recommendations to industry regarding cybersecurity device design, labeling, and the documentation that FDA recommends be included in premarket submissions for devices with cybersecurity risk. These recommendations can facilitate an efficient premarket review process and help ensure that marketed medical devices are sufficiently resilient to cybersecurity threats.
- Although FDA issued final guidance addressing premarket expectations in 2014 and a draft guidance in 2018,* the rapidly evolving landscape, and the increased understanding of the threats and their potential mitigations, necessitates an updated approach.

*FDA regularly replaces "final" guidances with new draft guidances

Device Cybersecurity Guidance (Draft)

- This guidance applies to all types of devices within the meaning of section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) **whether or not they require a premarket submission**. Therefore, the information in this guidance should also be considered for understanding FDA's recommendations for devices for which a premarket submission is not required (e.g., for 510(k)-exempt devices).

Device Cybersecurity Guidance (Draft)

- The changes proposed since the 2014 guidance are intended to further emphasize the importance of ensuring that devices are designed securely, are designed to be capable of mitigating emerging cybersecurity risks throughout the TPLC, and to more clearly outline FDA's recommendations for premarket submission information to address cybersecurity concerns.
- One way these TPLC considerations for devices can be achieved is through the implementation and adoption of a Secure Product Development Framework (SPDF). An SPDF is a set of processes that reduce the number and severity of vulnerabilities in products throughout the device lifecycle.

Device Cybersecurity Guidance (Draft)

- The recommendations in this guidance also generally align with or expand upon the recommendations in the Pre-Market Considerations for Medical Device Cybersecurity section of the International Medical Device Regulators Forum final guidance "Principles and 110 Practices for Medical Device Cybersecurity," issued March 2020
- *(FDA has increasingly been aligning with IMDRF guidances and standards)*

Device Cybersecurity Guidance (Draft)

- How does the revised draft compare with the 2018 draft?
  - Scope is much broader; applies to all medical devices, not just those requiring some type of approval process
    - Note, however, that the guidance does focus largely on requirements for pre-market submissions
  - "Cybersecurity Tiers" (Level 1 and 2 devices) are gone; all medical devices are subject to the same standards

Device Cybersecurity Guidance (Draft)

- About the only recognizable specific content from the previous draft (in definitions):
  - Trustworthy Device – a medical device that: (1) is reasonably secure from cybersecurity intrusion and misuse; (2) provides a reasonable level of availability and reliability; (3) is reasonably suited to performing its intended functions; and (4) adheres to generally accepted security procedures to support correct operation.

Table of Contents

What does all this have to do with telemedicine practice?

- The FDA's mantra: **We do not regulate the practice of medicine**
  - Clinical practice liability for telemedicine use of SaMD, AI/ML, etc., would be in the malpractice arena, under state licensing laws, or related to HIPAA obligations (or state privacy law) as a covered entity
- Be aware of which devices your telemedicine patients are using when you are incorporating device data into your telemedicine practice. Examples include
  - RPM devices directly communicating with the EHR or whose data are being organized into a dashboard communicating with the EHR
  - Patient uploads of their own diary data from devices

What does all this have to do with telemedicine practice?

- Are these devices FDA-cleared (if required)?
- What do the devices' cybersecurity labeling include?
- How does your own clinical privacy/security setup comply with HIPAA regarding the transfer and storage of device data?
- Are you able to independently review device data in a clinical decision-making situation?
  - Particularly important to the FDA with respect to its regulation of AI/ML decision support systems

Questions?