U.S. FOOD & DRUG ADMINISTRATION
CENTER FOR DEVICES & RADIOLOGICAL HEALTH

GLOSSARY FOR PATIENT ENGAGEMENT ADVISORY COMMITTEE MEETING ON CYBERSECURITY

TERMS	DEFINITION
Asset	The people, property, and information to be protected. In medical device cybersecurity, assets include the patient, the medical device, and data transmitted about the patient.
CDRH	Center for Devices and Radiological Health (CDRH) has the responsibility for protecting and promoting the public health through the approval of safe and effective medical devices.
CDRH Signal Management Program	Helps to ensure consistency, efficiency, accountability, and transparency in how CDRH evaluates and addresses signals related to marketed medical devices.
Class I Devices	Low risk devices requiring general controls to ensure safety and effectiveness.
Class II Devices	Requires general and special controls to ensure safety and effectiveness. Special controls may include guidance documents, mandatory performance standards, patient registries for implantable devices and postmarket surveillance. Requires a 510(k), unless exempted; may require clinical trials.
Class III Devices	Intended to be used in supporting or sustaining human life, or for a use which is of substantial importance in preventing impairment of human health, or that which may present a potential unreasonable risk of illness or injury, and for which insufficient information exists to determine that general controls and special controls are sufficient to provide reasonable assurance of the safety and effectiveness of a device.
Cloud	Computing resources (e.g., networks, servers, storage, applications, and services) that run on the internet instead of locally on your computer.
Compromised Privacy	Unauthorized access to patient or device information or data integrity.
Cybersecurity	Process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.
Cybersecurity Risk	When a vulnerability is confirmed to exist by manufacturers.
Cybersecurity Threat	When there is a possibility that a human or automated actor can successfully exploit a vulnerability.
Cybersecurity Vulnerability	When a potential concern is first identified.

U.S. Food & Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993
FDA.GOV

Electronic health records	An electronic version of a patient's medical history, that is maintained by the provider over time, and may include all the key administrative clinical data relevant to that person's care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, operative reports, and radiology reports.
Emerging Signal	Based on FDA's initial evaluation of new information which may have the potential to impact patient management decisions and/or the known benefit-risk profile of the device.
Exploit	Identifying and taking advantage of software vulnerabilities in medical devices leading to loss of authenticity, availability, integrity, or confidentiality.
Fit-for-purpose	The information is of sufficient quality to provide confidence in the analyses necessary to inform or support regulatory decision-making.
Health Literacy	Degree to which individuals have the capacity to obtain, process, and understand basic health information and services needed to make appropriate health decisions.
Internet of Things (IoT)	An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.
Informed Consent Form	Informed consent is a process by which a subject voluntarily confirms his or her willingness to participate in a particular trial, after having been informed of all aspects of the trial that are relevant to the subject's decision to participate. Informed consent is documented by means of a written, signed and dated informed consent form.
Interoperability	The ability of computer systems or software to exchange and make use of information.
Interconnected Devices	Devices capable of connecting (e.g., wired, wirelessly) to another medical or non-medical product, to a network, or to the Internet.
Interconnectivity	The ability to connect (e.g., wired, wirelessly) to a medical or non-medical product, to a network, or to the Internet.
Joint Security Plan	Describes best practices for implementing medical device cybersecurity and resilience recommendations, and further demonstrates the capabilities of medical device manufacturers working together with healthcare provider organizations to articulate a common vision to further safeguard patients.

Legacy Devices	Medical devices running outdated software that is unable to recognize or incorporate the security features.
Medical Device	An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component part, or accessory, which is: (1) recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them, (2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or (3) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. The term 'device' does not include software.
Medical Device Reports (MDRs)	A report submitted to the FDA by a manufacturer, a physician, or a patient about a marketed device that may have malfunctioned and/or caused or contributed to a death or serious injury. A report can be submitted at the following link: https://www.fda.gov/medicaldevices/safety/reportaproblem/default.htm.
Medical Device Safety Communication	Summary of the safety concern, recommendations for patients and caregivers, additional recommendations for health care providers, and the FDA's actions to resolve the safety concern.
Plain Language	Writing in a way that helps readers understand the content in a document the first time they read it.
Quality System Regulation	Provides the framework that all manufacturers must follow regarding organizational structure, responsibilities, procedures, processes, and resources for implementing quality management. In particular it governs the methods used in, and the facilities and controls used for, the design, manufacture, packaging, labeling, storage, installation, and servicing of all finished devices intended for human use. It is intended to ensure that finished devices will be safe and effective and otherwise in compliance with the Federal Food, Drug, and Cosmetic Act (the act).
Risk	The ***potential*** for loss, damage, or destruction of an asset which occurs when a threat exploits a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities. In medical device cybersecurity,

	the risk is typically associated with a hacker (threat) accessing a patient's device (asset) by exploiting a security weakness in the device's software or firmware (vulnerability).
Safety	Safety is relative freedom from harm. In clinical studies or in the real-world, this refers to an absence of harmful side effects resulting from use of the product and may be assessed by laboratory testing of biological samples, special tests and procedures, psychiatric evaluation, and/or physical examination of subjects.
Security Patches	Software changes that address cybersecurity vulnerabilities within the software to reduce the chances of exploitation.
Sensors	A device (not always a medical device) that detects and responds to some type of input from the physical environment including environment exposures (such as indoor smoke), location, physical activity (via accelerometry), sleep, social interactions, images, visual stimuli, glucose levels, and heart rhythms, with many more measures in development.
Signal	Represents a new potentially causal association or a new aspect of a known association between a medical device and an adverse event or set of adverse events.
Software	Programs, procedures, rules, and any associated documentation pertaining to the operation of a system.
Threat	Anyone or anything that can exploit a vulnerability, intentionally or accidentally, and steal, damage, or destroy an asset. In medical device cybersecurity, the threat is typically a "hacker," an unauthorized person who intentionally accesses and controls a device and uses that access to issue commands to the device.
Updates	Modifications to a medical device's software.
Vulnerability	A weaknesses or gap in a security program or protocol that can be exploited by threats to gain unauthorized access to an asset. In medical device cybersecurity, the vulnerability is typically associated with a security gap in the software or firmware used by the device.
Warning Letters	Notification the FDA sends to a manufacturer for violations of regulatory significance. They give the companies an opportunity to take prompt and voluntary corrective action before it initiates an enforcement action.