

October 12, 2023

Mass General Brigham maintains a high standard of system security in the operation of its clinical, administrative, and other information systems used by itself and its affiliated hospitals and organizations to support clinical care and clinical research.

Mass General Brigham has adopted a diversified range of access protocols, software solutions, technical safeguards, policies, monitoring and other systems and controls that are designed to maintain, as appropriate, the privacy, confidentiality, integrity and security of electronic clinical and research data. Mass General Brigham maintains a Privacy and Information Security Program, including policies, standards and procedures, and a security framework that meets recommendations of the International Organization for Standardization's (ISO) publication 27001 and the National Institute of Standards and Technology's (NIST) publication 800-53 Family of Controls and applicable regulatory and legal requirements and any related amendments or implementing regulations, as required (e.g., Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH)).

These systems and controls are designed for compliance with applicable laws as well as with industry standards set by leading academic medical institutions. With respect to 21 CFR Part 11 specifically, it is Mass General Brigham's understanding that FDA does not apply the Part 11 regulations to electronic health record systems ("EHRs") and does not intend to evaluate EHRs' compliance with Part 11's requirements, even when EHRs contain data relevant to clinical research.

Sincerely,



David Heaney
Chief Information Security Officer
Mass General Brigham