FDA AND HIPAA COMPLIANCE

Updated: 21 October 2018

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection. Anyone who deal with protected health information (PHI) must have physical, network, and process security measures in place and follow them to ensure HIPAA Compliance.

It is important to note that there is no certification recognized by the US HHS for HIPAA compliance and that complying with HIPAA is a shared responsibility between RECOMIA and our research partners. Specifically, HIPAA demands compliance with the Security Rule, the Privacy Rule, and the Breach Notification Rule. Our research forum supports HIPAA compliance, and our research partners are responsible for evaluating their own HIPAA compliance.

RECOMIA will enter into Data Processing Agreement with all researchers that use our research forum as necessary under HIPAA. Our forum is built and maintained with careful security consideration and details on our approach to security and data protection including details on organizational and technical controls regarding how RECOMIA protects data, can be found on recomia.org.

In addition to documenting our approach to security and privacy design, RECOMIA welcomes independent third party audits to provide clients with external verification.

FDA 21 CFT Part 11

RECOMIA adhere to 21 CFR Part 11 (part 11 of title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures). In brief, this document provides guidance to persons and suppliers who, in fulfilment of a requirement in a statute or another part of FDA's regulations to maintain records or submit information to FDA. The document sets out controls for closed systems like our research forum. In particular, it specifies how to protect records, limit system access (each user must have a username and password to gain access), use of secure and computer generated audit trails (sender, IDs, study type, time stamps, etc.), perform authority checks to prevent unauthorized access, how to establish and adhere to written policies such as research protocols.

Part 11 Section 11.10a states: "Control for closed systems are to include the validation of systems to ensure accuracy, reliability, consistent, intended performance, and the ability to conclusively discern invalid or altered records" . Our validation is based on two principles: data integrity and standards conformance. We protect the integrity of the data we process through robust data encryption throughout the entire data collection and transfer process. Any change to the encrypted data will be flagged as incomplete and rejected due to the potential safety breach. Standards conformance ensures that RECOMIA will automatically reject any file that does not meet the DICOM conformity specification outlined in the necessary research protocol. This ensures that only DICOM files meeting your data requirement are collected and transferred to our research forum.

Part 11 Section 11.10(e) states: "Audit trails must be secure, computer-generated and timestamped to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. Audit trails should say 'who did what to your records and when." All operations performed on our research forum are logged carefully to ensure compliance with section 11.10(e), and includes user, institution, type and size of study incl. IDs, number of images, number of series, resolution parameters, and timestamps. All transfer logs are securely kept for future audits.