Indiana University Health, Inc. Guidelines on International Data Usage

The purpose of this exhibit is to set the requirements and guidelines by which IU Health data can be accessed by foreign third parties outside the United States and Canada. Due to the increased risk of data exfiltration and low enforceability of agreements across borders, IU Health has put these requirements and guidelines into place to protect stakeholders.

i. Data Hosting Location. IU Health data must be hosted in the United States, Canada, or a mutually agreeable location where data will be protected under appropriate privacy laws. IU Health will approve the ultimate destination(s) of data.
   a. If data is stored in a mutually agreeable location, the appropriate supervisory authorities will be contacted and advised. Appropriate documentation, such as a Data Protection Impact Analysis and supporting documentation under the European Union General Data Protection Regulation (GDPR) will be filed with them and shared with IU Health.
   b. Whenever possible, data stored outside the United States will be verified and validated using distributed technologies and cryptographic hashing used to keep copies of the hashes in multiple locations, including locations within the United States, even if the data itself resides outside the US.
      i. Distributed systems used to store these hashes must meet IU Health security requirements, detailed in the Indiana University Health Verification and Validation using Distributed Computing Requirements appendix.

ii. Data Access. Access to data outside the United States, Canada, or the agreed-upon location will be via remote or virtual desktop technology using two-factor authentication based upon strong cryptography using technology agreed upon by the vendor and IU Health.
   a. Text message-based authentication is not allowed due to interception risk.
   b. Devices used to access data must meet or exceed IU Health Security Standards

iii. Data Processing. IU Health data must be processed and/or have analytics performed on it in the United States, and the results of the analytics must be stored there.

iv. Data Security. Data stored outside the United States must be stored in facilities that are ISO 27001 certified.

v. Cloud Security. Data stored outside the United States with Cloud providers must be stored with ISO 27017/27018 certified providers. The provider must be certified for the region(s) the data will be stored in.

vi. Restricted Countries and Entities. IU Health forbids Business Associate or any of its subcontractors or subservice providers from directly employing resources or contracting for services on its behalf from countries on the US Department of the Treasury Office of Foreign Asset (OFAC) Control Sanctions Programs list, available at https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx. IU Health also forbids Business Associate or any of its subcontractors or subservice providers from directly employing resources or contracting for services on its behalf from people or companies on the US Commerce Department Bureau of Industry and Security Consolidated Screening List, available at: https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern