Applicability: UW Medicine[1] and UW Medicine Affiliated Covered Entity[2]

Policy Title: Offshore Storage of and Access to UW Medicine Data by Third Parties

Policy Number: COMP.305

Superseded Policies: N/A

Date Established: August 16, 2024

Date Effective: August 16, 2024

Next Review Date: August 16, 2027

PURPOSE

To describe under what circumstances UW Medicine data may be stored or accessed by individuals outside of the United States (hereafter referred to as "offshore") and, when permitted, the related measures that must be undertaken to demonstrate the privacy and security of such storage or access. Specifically, this policy is intended to address the following primary use cases:

1. Offshore storage of UW Medicine data; and
2. Offshore access to UW Medicine data by third parties/vendors.

Access to UW Medicine data by UW Medicine workforce members while working offshore is governed by the UW Medicine Acceptable Use Standard.

[1] UW Medicine is an integrated clinical, research and learning system with a single mission to improve the health of the public. The clinically integrated parts of UW Medicine consist of the following:

- Airlift Northwest
- Fred Hutchinson Cancer Center (* Please note, the UW Medicine Compliance Program and this policy apply to UW faculty. Fred Hutch employees who are not also UW faculty are required to comply with Fred Hutch compliance policies only.)
- Harborview Medical Center
- UW Medical Center
- UW Medicine Primary Care
- UW Physicians
- UW School of Medicine
- Valley Medical Center

[2] The University of Washington (UW) is a hybrid covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), comprised of healthcare and non-healthcare components. For the purposes of HIPAA, the UW has designated healthcare components, and further designates a group of healthcare components to be one affiliated covered entity known as UW Medicine Affiliated Covered Entity (UW Medicine ACE). Healthcare components of the UW Medicine ACE are represented in 101.G1 University of Washington (UW) HIPAA Designation – *UW Medicine – Affiliated Covered Entity.*

DEFINITIONS

A. "De-identified Health Information" means data that has been de-identified in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")(see Section, VI(B) of COMP.103, Uses and Disclosures of Protected Health Information).

B. "Protected Health Information" (PHI) means information (verbal, paper, or electronic) maintained or transmitted by UW Medicine that relates to:
   - The past, present, or future physical or mental health or condition of an individual;
   - The provision of healthcare to an individual; or
   - The past, present or future payment for the provision of healthcare to an individual and either a) identifies the individual or b) provides a reasonable basis to believe the information can be used to identify the individual.

C. "Research Data" means data that has been derived from UW Medicine clinical data and has been collected or created through research and is maintained as part of a research record.

D. "UW Medicine Data" means the following types of data stored in any UW Medicine system or application:
   - Clinical data. For purposes of this policy, Clinical data is data created or received by UW Medicine in clinical care decision making, provision, billing or payment. Clinical data includes healthcare delivery records (including PHI), provider data, de-identified healthcare data, data utilized for Quality Improvement activities, metadata, reference data, healthcare supply chain data, laboratory data, referral data, patient-level financial data, other forms of confidential or sensitive data within healthcare records or databases of UW Medicine (including metadata and reference data);
   - Financial data;
   - Employee data;
   - Research Data derived from UW Medicine clinical data; and
   - Any other data used for UW Medicine business, clinical or operations purposes.

   For the purposes of this policy, UW Medicine Data *does not* include UW Medicine information published for public use or has been approved for public use by an appropriate University of Washington authority (see UW Administrative Policy Statement 2.4).

E. "UW Medicine Workforce Member" means an employee, trainee, volunteer or role-specific contractor whose performance is under the direct control of a clinically integrated part of UW Medicine.

POLICY

Offshore storage of and access to UW Medicine Data must comply with all relevant UW Medicine Compliance Patient Information Privacy policies and UW Medicine Information Security Standards. Because of the heightened privacy and security risks associated with offshore storage and access, the procedures described in the next section must be followed to identify such risks, implement privacy and security controls to reduce risks to an acceptable level, and escalate proposed offshore arrangements to leadership for approval when appropriate.

Offshore storage of and access to UW Medicine Data may be considered in the following circumstances:

A. UW Medicine contracts with a US-based third party that has offshore satellite offices, employees.
B. UW Medicine contracts with an offshore third party with limited presence in the US.
C. An IRB-approved research project that involves offshore collaborators and data sharing which complies with UW Medicine policies, the executed Data Use Agreement, the research protocol, UW Office of Research standards and any other obligations associated with conducting the research (e.g., study sponsor requirements).

Offshore storage of and access to UW Medicine Data will not be considered in the following circumstances:

A. UW Medicine may not provide direct access to an application containing UW Medicine Data (e.g., Epic) with an offshore third party.
B. UW Medicine has a contract with a US-based vendor and the vendor seeks to subcontract work involving UW Medicine Data to an offshore subcontractor that has no physical presence in the United States.
C. Offshore storage or access arrangements involving countries deemed safety risks by the UW Medicine Information Security Program.
D. Offshore storage or access arrangements that would violate an existing contractual obligation or other restriction (e.g., Epic, Boeing ACN).
E. When the offshore storage or access arrangement includes clinical data received as part of the Clinical Data Exchange Memorandum of Understanding between Fred Hutchinson Cancer Center and the University of Washington unless written approval is obtained from the Joint Clinical Data Oversight Committee or the data sharing occurs pursuant to a mutually agreed upon written offshore data policy.

PROCEDURES

A. Data domain steward approval. Data domain stewards must approve offshore arrangements. Examples include:
    1. Clinical data must be approved by the Senior Director of Enterprise Records and Health Information.
    2. UW Medicine financial data must be approved by the office of the Chief Financial Officer or delegate.
    3. UW Medicine employee data must be approved by the appropriate Director of Human Resources for the UW School of Medicine or Hospital and Clinics.
    4. UW research data must be approved by the principal investigator, the Vice Dean of Research and Graduate Education, the UW Office of Sponsored Programs (when applicable), or other appropriate institutional official.
    5. For any other data used for UW Medicine business, clinical or operational purpose, the Clinical Business and Regulatory Affairs Officer shall be consulted to identify the appropriate data domain steward to approve the offshore arrangement.

B. Contract Requirements.
    1. After the business owner's approval is confirmed, a written agreement must be executed before granting offshore storage or access to UW Medicine Data to a third party.

2. The written agreement must be drafted and reviewed by the Attorney General's Office or the appropriate contracting team (e.g., UW Procurement, UW Medicine Supply Chain, Clinical Business and Regulatory Affairs, etc.) to identify risks and ensure contractual safeguards are in place before offshore storage or access to UW Medicine Data is permitted.
3. The agreement must include an IT Rider. Changes to the IT Rider are reviewed and approved by UW Medicine ITS.
4. A Business Associate Agreement (BAA) must be executed if the arrangement involves UW Medicine PHI and the data recipient meets the definition of a business associate. UW Medicine Compliance must review the BAA before offshore storage or access to UW Medicine PHI is permitted.
5. Any applicable storage maintenance agreements must be terminated at the close of the relationship with UW Medicine.

C. Privacy and Security Assessments.
UW Medicine Compliance and the UW Medicine Information Security Program must review any arrangement in which this policy applies to assess the level of risk it would pose to the organization. As appropriate, the UW Medicine Information Security Program will conduct an initial and periodic assessment of the security controls in place.

D. Escalation Process.
If UW Medicine Compliance, the UW Medicine Information Security Program or applicable legal team identify significant risks concerning a proposed offshore arrangement, the following escalation pathways will be used depending on the nature of the risk:
1. Operational business risks will be reviewed by the business owner
2. IT business risk will be reviewed by the UW Medicine Chief Information Officer.
3. Compliance or legal risks will be reviewed by the Compliance Governance Group.
4. Information security risks will be reviewed by the Security Program Executive Committee.

E. Document Retention.
All official records, including superseded policies, are retained in accordance with applicable records retention policies.

REGULATORY/LEGISLATION/REFERENCES

- Security Standards for the Protection of Electronic PHI, 45 C.F.R. § 164, Subpart C.
- Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164, Subpart E.
- https://www.hhs.gov/hipaa/for-professionals/faq/2083/do-the-hipaa-rules-allow-a-covered-entity-or-business-associate-to-use-a-csp-that-stores-ephi-on-servers-outside-of-the-united-states/index.html.

PROCEDURE ADDENDUM(s) REFERENCES/LINKS

- UW Medicine Compliance Patient Information Privacy Policies: https://depts.washington.edu/comply/privacy-policies/
- UW Medicine Information Security Standards: https://depts.washington.edu/uwmedsec/restricted/security-governance/information-security-standards/

APPROVALS

/s/ Beth DeLair 8/22/2024

Beth DeLair
Chief Compliance Officer, UW Medicine
Associate VP for Medical Affairs, UW

Date