DATA SECURITY PLAN CANONIC Community Learning Study

2026-03-18

Dexter Hadley, MD/PhD

Hadley Lab CANONIC

hadleylab.org Governed Document. Every claim cited.

0.1. 1. Data Classification

The community learning ledger is classified as **non-identifiable research data**. The data schema contains no personally identifiable information by design. Each ledger entry consists of three fields: date, question text, and a random session identifier. No linkage table exists to connect session identifiers to any individual.

0.2. 2. Storage

Layer	Mechanism
Primary	CANONIC governed repository, version-controlled, append-only
Integrity	Cryptographic hashing of all evidence records
Immutability	Append-only ledger architecture; entries cannot be modified or deleted
Access	Role-based access controls governed by CANONIC framework

---

0.3. 3. Access Controls

Access to the community learning ledger is restricted to:

1. Principal Investigator (Dexter Hadley, MD/PhD)
2. Co-Investigator (Marisa Nimrod, MD)
3. CANONIC Foundation governance administrators

No third-party access is granted. No data sharing agreements exist. Aggregate results are published; raw ledger entries are not shared outside the research team.

0.4. 4. Transmission

Ledger data is transmitted exclusively over encrypted channels. The CANONIC governance framework enforces HTTPS for all service endpoints. No unencrypted transmission of ledger data occurs at any point in the data lifecycle.

0.5. 5. Retention

The community learning ledger is retained permanently. It is the institutional memory of the community learning system. Retention is governed by the append-only architecture: entries cannot be deleted because deletion would compromise the integrity of the community intelligence.

0.6. 6. Breach Response

In the event of unauthorized access to the governed repository:

1. The append-only ledger is cryptographically verifiable; any tampering is detectable.
2. No PII exists in the data; a breach of the ledger would expose only anonymized questions.
3. No linkage table exists; exposed data cannot be connected to any individual.
4. The IRB will be notified within 72 hours of any detected unauthorized access.

The risk classification for a data breach is **minimal** because the data is structurally non-identifiable.

IRBS | CARIBCHAT | SECURITY | 2026-03-18