The CIA-HDL Matrix

Extending the CIA triad across Human | Digital | Legal℠ domains

The CIA triad — Confidentiality, Integrity, and Availability — is a foundational model for information security. It identifies three core information-security objectives organizations must protect.

In practice, issues involving the three CIA elements rarely remain confined to digital systems. They almost invariably intersect with three domains:

- **Human —** effects on patients, clients, workers, vendors, and sometimes the public; behavior, workflow, communication, and operational trust.
- **Digital —** systems, access, data flows, technical controls, logs, alerts, automation, backups, and data recovery.
- **Legal —** statutory and regulatory obligations, privacy duties, availability duties, liability exposure, notification requirements, and accountability.

Purpose

The CIA-HDL Matrix provides a visual structure for organizing each element of the CIA triad across Human, Digital, and Legal domains. The framework gives leadership a governance structure while giving frontline team members a way to contribute meaningfully to it. It converts workflow problems, observations, and proposed fixes into organized governance input, then converts governance decisions back into clear ownership, controls, workflows, documentation, escalation, communication, and corrective action.

Example: Ransomware in a Healthcare Organization

A ransomware attack may affect all three CIA elements:

- **Confidentiality:** patient information is exposed.
- **Integrity:** records are altered, corrupted, incomplete, or unreliable.
- **Availability:** access to systems, data, or operational workflows is interrupted.

The matrix maps these issues across Human, Digital, and Legal domains:

	Human	Digital	Legal
Confidentiality	Patient distress; loss of trust	PHI exposed or exfiltrated	HIPAA/privacy duties; breach analysis; notification exposure
Integrity	Unsafe care decisions	Altered, corrupted, or incomplete records	Malpractice exposure; record-integrity and evidentiary issues
Availability	Delayed care; diversion; workflow disruption	EHR, portal, ordering, scheduling, or backup systems unavailable	Continuity duties; regulatory and contractual exposure

In this case, the CIA-HDL Matrix shows how the three CIA elements become human effects, digital conditions, and legal/accountability consequences. It gives frontline team members a structure for communicating concerns and proposed fixes, while giving leadership a structure for assigning ownership, safeguards, evidence, recovery work, and remediation.

Primary Uses

- **Governance —** assign ownership, decision rights, escalation paths, communication duties, documentation expectations, and accountability.
- **Controls and Audit —** translate mapped risks into control requirements, evidence expectations, testing activity, exception documentation, audit posture, and remediation.
- **Resilience and Corrective Action —** organize what must happen before, during, and after disruption: planning, role assignment, downtime procedures, recovery work, root-cause analysis, corrective action, and communication back to affected people.

Conclusion

By organizing the three CIA elements across Human, Digital, and Legal domains, the CIA-HDL Matrix turns the CIA triad into a practical structure for governance, controls, and operational resilience. It works in both directions: team members convert lived workflow problems, observations, and proposed fixes into governance-relevant input; leadership converts governance decisions back into ownership, controls, workflows, documentation, escalation, communication, and corrective action. This preserves the value of frontline experience while giving leadership a structure for making, documenting, and communicating decisions.

Mark Yoffe, MD, CISSP | linkedin.com/in/mark-yoffe-md-a9927956