Legacy reliance and HIPAA Privacy & Security Requirements in the US Health Care Industry.

The Nature of Legacy Systems
US hospitals and healthcare networks depend heavily on **legacy medical equipment and IT infrastructure.**

These systems include:

- Diagnostic and imaging equipment (MRI, CT, X-ray) running on outdated operating systems (Windows XP, 7, or even proprietary OSs)
- Laboratory and pharmacy systems built on old client-server or mainframe architectures
- Networked medical devices (infusion pumps, ventilators, patient monitors) with **hardcoded firmware** and minimal cybersecurity controls
- Electronic Health Record (EHR) systems with limited patch ability and outdated interfaces

Many of these devices are **regulated medical products**, which complicates or prohibits software modifications without FDA re-certification — leading to long lifecycles (10–20+ years).

Result: Noncompliance can lead to severe consequences:

- Civil penalties up to **$1.9 million per year per violation category (as of 2025 adjustments)**
- Reputational harm and patient trust erosion
- Significant breach remediation costs — the **average cost of a healthcare data breach** now exceeds **$10 million**, the highest of any industry (*IBM, 2024*)

The Strategic Path Forward
Most healthcare organizations are adopting **risk-based modernization strategies** rather than wholesale replacement, but there is another option, one that extends the life of the medical equipment, helps with regulatory compliance and can protect medical data without changing the medical device.

Certes DPRM (Data Protection and Risk Mitigation) is a data protection solution that ensures data flowing from any medical device over an IP network is protected in a form that is only accessible by the data owners and no one else, no matter where that data travels. It works on individual data flows providing each with its own protection policy, encryption key and rotation schedule of that key. Each application data flow then becomes invisible to any other, this makes DPRM ideal for segmentation and isolation at the data level without complex and expensive network architectural changes or wholesale replacement of medical equipment. For IoT devices within the medical establishment (such as CCTV cameras, security devices etc.), DPRM can also be deployed to secure and protect those data/control streams and keep them separate from any other network traffic.

In Summary
Certes DPRM provides the US Health Care sector with a simple, cost-effective way to comply with modern data protection regulations with a solution that is transparent to all other network / monitoring devices, extends the life of legacy systems, reduces risk and potentially reduces the Cyber related costs associated with a data breach.

In the next few pages, we compare the Regulatory requirements of HIPAA, HIPAA Security and HIPAA Privacy with the capabilities of DPRM.

This table summarizes key HIPAA Privacy and Security Rule requirements and compares them to the capabilities of Certes' DPRM solution. It also highlights customer-owned responsibilities where DPRM is not sufficient by itself. This is a practical mapping, not legal advice.

Requirement	What HIPAA Requires	How Certes DPRM Helps	Gaps / Customer Responsibilities
Permitted uses & disclosures; Authorizations	Limit PHI use/disclosure to treatment, payment, health care operations; obtain written authorization for other uses. Apply minimum necessary. Provide Notice of Privacy Practices (NPP).	DPRM focuses on data-centric protection (encryption/crypto-segmentation) that can enforce policy at flow level; helps ensure only authorized flows can access protected payloads. DPRM ensures data is protected and sovereign at all times.	DPRM does not manage legal bases, consent/authorizations, NPP distribution, or "minimum necessary" determinations. Covered entity policies and workflows are required.
Individual rights (access, amendment, accounting, restrictions, confidential communications)	Provide processes to respond to requests for access, amendments, restrictions, and confidential communications; maintain accounting of certain disclosures.	Encryption and centralized policy/key management can help segregate datasets to facilitate access controls and audit at the data-flow level.	Request intake, fulfillment, disclosure accounting, and record management remain operational/legal processes outside DPRM's scope.
Administrative requirements & workforce training	Designated Privacy Officer; adopt policies/procedures; train workforce; complaint process.	Can supply technical controls to support policies (e.g., segmentation by role or application).	Governance, org training, and privacy administration are customer responsibilities.
Business Associate Agreements (BAAs)	Execute BAAs with vendors handling PHI and ensure appropriate safeguards.	DPRM's separation of duties and customer-owned keys can reduce vendor risk and support BAA-required safeguards.	Negotiating/maintaining BAAs and vendor oversight remains with the covered entity/business associate.

HIPAA Security Rule (45 CFR Part 164 Subpart C): How DPRM Maps

Requirement	What HIPAA Requires	How Certes DPRM Helps	Gaps / Customer Responsibilities
Risk analysis & risk management (Administrative)	Conduct an enterprise risk analysis of ePHI and implement risk management measures; periodic reviews.	DPRM adds data-centric controls (crypto-segmentation, quantum-safe encryption) and centralized key/policy management to reduce data in motion risk.	Formal risk analysis methodology, documentation, and enterprise risk register are outside the tool; customer must perform and evidence them.
Workforce security; information access management (Administrative)	Authorize/establish access to ePHI based on role; supervise workforce; terminate access.	Enforces policy at the data-flow level; integrates with key/policy rotation to time-bound access.	Identity lifecycle (HRIS/IdP), role definitions, joiner/mover/leaver processes and MFA are outside DPRM—must be handled by IAM.
Security incident procedures & response	Identify, respond to, mitigate, and document incidents.	Centralized reporting on protected flows can aid detection/containment; encryption reduces impact.	IR playbooks, forensics, breach assessment, and regulatory notifications are customer responsibilities.
Contingency planning (backup, disaster recovery, emergency mode)	Create/test data backup, DR, and emergency operations plans.	Encryption and key management can be incorporated into backup/DR architectures.	Backup tooling, restoration testing, RTO/RPO design, and DR runbooks are beyond DPRM.
Facility access controls; workstation security (Physical)	Limit physical access to systems/facilities; secure workstations and devices.	Not a physical control; encrypted data reduces exposure if devices/networks are compromised.	Badges, locks, cameras, endpoint hardening/MDM remain required.
Device & media controls (Physical)	Policies for disposal, media re-use, data movement.	Encryption helps render data unreadable on decommissioned media when keys are destroyed/rotated.	Sanitization procedures and chain-of-custody are customer tasks.
Access control (Technical)	Unique user IDs, emergency access procedures, automatic logoff, encryption when reasonable and appropriate.	Provides crypto policy enforcement and segmentation at Layer 4; centralized key and policy control; FIPS/Common Criteria-certified versions available.	User-level authN/Z, MFA, session management, and app-layer controls require IAM/EDR/EHR controls.
Audit controls (Technical)	Record and examine activity in systems containing ePHI.	Centralized policy management and flow reporting provide security telemetry for protected flows.	SIEM integration, log retention, correlated audit across apps/databases still needed.
Integrity (Technical)	Protect ePHI from improper alteration or destruction.	Cryptography can protect payload integrity during transit and at rest as part of policy.	App/database integrity controls (checksums, immutability, WORM storage) are separate.
Transmission security (Technical)	Protect against unauthorized access during transmission (e.g., encryption).	Applies payload protection and crypto-segmentation across networks independent of transport; supports key rotation.	Email/SFTP configuration hygiene still required where applicable.

Breach Notification Rule (45 CFR 164.400–414)

Requirement	HIPAA Expectation	How DPRM Helps / Note
Individual & HHS Notification	Notify affected individuals without unreasonable delay and no later than 60 days after discovery; report to HHS (immediately for 500+).	Strong encryption and key control can qualify data as "unsecured" vs. "secured"; if data is encrypted to NIST standards and keys are not compromised, breach notification obligations may not be triggered (per risk assessment).
Media Notification (500+)	If 500+ individuals in a state/jurisdiction, notify prominent media in 60 days.	DPRM reduces likelihood of "unsecured" PHI disclosure by rendering exfiltrated data unintelligible.
Business Associates	BAs must notify covered entities of breaches.	DPRM's separation of duties and customer-owned keys can reduce BA exposure; contract terms still required.

Notes & Assumptions

• **Jurisdiction:** HIPAA is U.S. federal law. Canadian healthcare generally follows PIPEDA and provincial laws (e.g., PHIPA in Ontario); this document focuses on HIPAA.

• "Certes DPRM" capabilities summarized here are based on publicly available product information and may vary by version/deployment.

• This mapping highlights where DPRM supports specific safeguards and where additional controls/processes are required.

"Certes DPRM can reduce risks, costs and help US Health Care sector comply with regulations without wholesale Rip and Replace of equipment"

certes.ai
+1-412 262 2571
info@certes.ai