RegenMed

WHITE PAPER

PERSONAL HEALTH INFORMATION: FROM CUSTODIANSHIP TO SOVEREIGNTY

February 2026

TABLE OF CONTENTS

MACRO THESIS: DISSOLUTION OF ADMINISTRATIVE DATA

The healthcare ecosystem has reached a structural inflection point where the legacy paradigms of data "ownership" and "de-identification" have collapsed. This failure is not a localized technical glitch but a systemic obsolescence of the foundational logic that has governed health information technology (IT) since the inception of the Health Insurance Portability and Accountability Act (HIPAA).

In the current 2026 landscape, the industry is navigating the "veracity mandate", a regulatory and operational requirement that administrative claims data—historically the lifeblood of health research and payer analytics—be replaced by high-trust evidence derived from clinical truth.

For decades, the market has operated on the "data exhaust" model, where clinical information was treated as a byproduct of billing processes. This administrative data, however, lacks the proven medical accuracy required for the high-stakes environment of 2026, characterized by the FDA's acceleration toward 60-day reviews for life-critical therapies and the total removal of switching studies for biosimilars.

In such an environment, the burden of proof has shifted from government oversight to the data itself. The structural solution is the implementation of clinical rules and data standards before the patient visit, making billing errors and protocol deviations technically impossible. This ensures the production of "verified facts ready for review", a baseline requirement for any organization seeking to maintain a Higher Business Valuation in a tech-enabled asset class.

Strategic Metric	Administrative Claims Model (Legacy)	Veracity Mandate Standard (2026)
Data Integrity	High noise; subject to billing lag and error.	Proven Medical Accuracy; protocol-enforced.
Verification Speed	Months to years (Audit-based).	Real-time (Verified Facts Ready for Review).

Regulatory Burden	High (Periodic static assessments).	Low (Continuous automated auditing).
Primary Utility	Reimbursement justification.	High-Trust Evidence for Licensing and RWE.
Economic Logic	Data Brokerage (Siloed enrichment).	Self-Sovereign Identity (Patient Licensing).

The transition from "data custodianship"—where hospitals and other institutions hold data in restrictive silos—to "self-sovereign health identity" (SSI) is the essential strategic response to this shift. Under the SSI framework, the patient transitions from being a passive data subject to the active sovereign of their clinical identity, licensing identified longitudinal data directly to researchers.

This transition is underpinned by RegenMed's Circles Platform, built to enable a dual-token model consistent with the GENIUS Act of 2025. This in turn supports automated settlements, thereby achieving an approximate 70% reduction in Real-World Evidence (RWE) procurement costs.

HIPAA ACCESS RIGHTS VS. STATE PROPERTY LAWS

A critical friction point in the modern healthcare economy is the divide between federal patient access rights and state-level business property laws. While many healthcare executives operate under the dry legal technicality that hospitals and physician groups "own" medical records as business assets, this ownership is increasingly hollowed out by the federal right-of-access provision.

The HIPAA Access Right and the "Bundle of Rights"

Under 45 CFR 164.524, an individual has a legally enforceable right to inspect and obtain a copy of their protected health information (PHI) in a "designated record set" for as long as that information is maintained. This right is absolute, with very few exceptions such as psychotherapy notes or information compiled for legal proceedings. Indeed, the 2025 and

2026 regulatory environment has seen a heightened focus by the Office for Civil Rights (OCR) on the "Right of Access Initiative," which treats the failure to provide records in a timely manner as a primary violation subject to massive civil monetary penalties.

Federal enforcement has clarified that, while a hospital may own the physical hard drive or the cloud-based database architecture, the patient possesses a "bundle of rights" that effectively controls the data's utility. In 2025, OCR announced its 53rd enforcement action under this initiative, imposing a $200,000 penalty on an academic medical center for failing to provide timely access. Other notable cases include Oregon Health & Science University, which faced a $200,000 fine for imposing unlawful access barriers and charging prohibited retrieval fees.

State Property Law and the "Custodianship" Trap

State laws generally assign the ownership of the physical medical record to the healthcare provider who created it. However, the legal analysis for 2026 indicates that this "ownership" is more akin to custodianship than traditional property ownership.

Because federal law (HIPAA and the 21st Century Cures Act) mandates the frictionless transfer of this data at the patient's request, the hospital's ability to "monetize" the data without patient involvement is legally and technically constrained. The "unjust enrichment" of data silos—where institutions sell de-identified patient data to brokers—is being actively challenged by patient advocacy groups and new state privacy mandates.

The conflict between these jurisdictions creates a liability trap for healthcare organizations. Relying on state property law to sell data without explicit patient licensing exposes healthcare institutions, (including Management Services Organizations) to information blocking penalties and private lawsuits, especially as de-identification protocols are proven obsolete.

Regulatory Authority	Statutory Reference	Executive Implications
Federal Access Rights	(https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.524)	Mandates 30-day response time; prohibits retrieval fees for

		patients.
Information Blocking	(https://www.healthit.gov/topic/information-blocking)	Penalties up to $1 million for practices interfering with EHI access.
State Privacy Laws	Varies (e.g., TASAA in TX)	Permits private lawsuits for data misuse starting Jan 1, 2026.
DOJ Bulk Data Rule	(https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern)	Restricts bulk transfer of genomic/biometric data to "countries of concern".

THE MOSAIC EFFECT DEEP DIVE—THE END OF ANONYMITY

The central technical justification for the transition to SSI is the total collapse of the de-identification "safe harbor" protocol. Historically, HIPAA's de-identification standard (removing 18 specific identifiers) was considered sufficient to protect patient privacy. However, the "mosaic effect"—the process of combining disparate, seemingly innocuous data points to reveal a unique individual fingerprint—has rendered this standard obsolete.

The Mechanism of the Mosaic Effect

In the 2025/2026 data ecosystem, re-identification no longer requires a name or social security number. Instead, the layering of longitudinal clinical journeys (e.g., a specific sequence of diagnoses and treatments), ZIP+3 location data, and precise clinical dates creates a biometric fingerprint. Research has demonstrated that a combination of just three variables—gender, postal code, and date of birth—is sufficient to uniquely characterize 87% of the U.S. population.

In healthcare, this effect is amplified by Social Determinants of Health (SDoH) markers and behavioral data. When a clinical record is "mosaicked" with external datasets—such as voter registration lists, property records, or social media activity—the anonymity of the clinical record vanishes. 2025 case studies from Vanderbilt University Medical Center and other institutions have utilized "adversarial modeling" to show that re-identification risk is situationally dependent; as the abundance of auxiliary data grows, the "expert determination" of anonymity becomes a transient and ultimately unreliable metric.

Linkage Attacks: 2025/2026 Evidence

A "linkage attack" occurs when an adversary possesses an auxiliary table with explicit identifiers and overlapping quasi-identifiers, allowing them to match records and re-identify individuals in a supposedly anonymous dataset.

2026 research indicates that large language models (LLMs) like GPT-5 have developed semantic inference capabilities, enabling them to infer a patient's identity from the narrative context of clinical notes even after all structured PII has been redacted.

Attack Type	Mechanism	Technical Reality (2026)
Direct Linkage	Matching QIs (age, sex, ZIP) across datasets.	High success rate due to external data abundance.
Semantic Inference	LLMs inferring attributes from narrative context.	GPT-5 reduces semantic leakage but smaller models fail.
Membership Inference	Determining if a record exists in a training set.	Poses risks to the integrity of AI-driven research.
Mosaic Reconstruction	Building a longitudinal journey from fragments.	Renders Safe Harbor de-identification "dry technicality".

This technical reality means that any organization selling "de-identified" data is essentially selling a "pre-identified" asset with a delayed detonation. The transition to SSI and

identified patient licensing is the only technical response that aligns the legal framework with the mathematical reality of modern data science.

The Genomic Paradox and the Failure of Expert Determination

Genomic data represents the ultimate challenge to the custodianship model, creating what is known as the "genomic paradox." Unlike a medical record which describes a state of being, a genomic sequence is the definition of the individual. The sequence *is* the identity; it cannot be changed, and it cannot be truly anonymized.

Identifiability as a Biological Constant

Research into pangenome graphs in 2026 has shown that as genomic resources expand, the ability to obfuscate haplotype paths without destroying the data's utility is diminishing.

Tools like "PanMixer" attempt to balance privacy and utility, but linkage attacks remain robustly successful against even these advanced methods. Because of the inherited nature of the genome, the re-identification of one individual can potentially compromise the privacy of an entire lineage, creating "collective privacy risks" that traditional individual-centric consent models fail to address.

The National Institutes of Health (NIH) recognized this by proposing a modernized Genomic Data Sharing (GDS) Policy. The revision simplifies thresholds for "large scale" genomic data to include any study with 100 or more individuals, mandating strict consent and data sharing requirements. Crucially, the NIH is moving toward "Controlled-Access Data Repositories" because "open medical data is a dying concept if not already dead".

The Failure of Expert Determination

HIPAA's "expert determination" method allows for de-identification if a statistical expert certifies that the risk of re-identification is "very small". However, in the genomic context, this determination is functionally invalid for permanent anonymity. An expert can only certify that the risk is low *given current external datasets*. As more genomic data is published (e.g., through consumer ancestry sites), the "small risk" of 2024 becomes a "near certainty" by 2026.

The Genomic Paradox necessitates the RegenMed SSI model: if the data cannot be anonymized, the only ethical and legal pathway is identified, sovereign licensing. By treating

the patient as the owner of their genomic dividends, the system replaces the myth of anonymity with the reality of sovereignty.

THE REGENMED SSI SOLUTION—THE "SPLIT-IP" MODEL

The transition to Self-Sovereign Health Identity requires a new contractual and technical architecture that acknowledges the tripartite interests in healthcare data. This is codified in the "Split-IP" Model, a fundamental logic that redistributes ownership and economic benefits.

Defining the Split-IP Framework

In the legacy custodianship model, the institution attempted to claim all rights. In the Split-IP model, the intellectual property (IP) is disaggregated to align with the actual value creation:

- **The Practice owns Source Data:** The clinical entity (the physician or medical group) retains ownership of the raw clinical records. This is necessary for malpractice protection, state-mandated record retention, and the provision of ongoing care.
- **The Platform owns AI Weights:** The technology provider (RegenMed) owns the computational intelligence—the "weights"—derived from analyzing massive, multi-institutional datasets. The platform provides the infrastructure for proven medical accuracy and high-trust evidence.
- **The Patient owns Sovereignty and Dividends:** The individual patient remains the ultimate sovereign of his/her identity. They hold the right to license their identified longitudinal data for secondary research and receive automated data dividend payments – Circle Health Coins (CHCs).

The End of Unjust Enrichment

This model resolves the "unjust enrichment" dilemma that has plagued the health data market. Currently, data brokers and large health systems extract billions in value from patient data without returning a single cent to the source. The SSI framework, powered by

the Circles Platform, ensures that patients are fairly compensated for their participation in clinical research.

This alignment of interests increases data quality and participant retention, as patients are incentivized to maintain a longitudinal clinical identity rather than a fragmented set of records.

Ownership Layer	Responsible Entity	Strategic Utility
Source Data	Clinical Practice	Regulatory Compliance / Care Delivery.
AI Weights	Platform (RegenMed)	High-Trust Evidence / Algorithm Transparency.
Identity/Dividends (Circle Health Coins)	Patient	Ethical Research / Economic Participation.

Financial Mechanics

The ability to settle CHCs at scale requires a financial infrastructure that operates at the speed of clinical verification. The Circles Platform is designed to operate within the proposed regulatory frameworks such as the Data Care Act of 2025 (S.3570), currently pending in the U.S. Senate.

The Dual-Token Mechanics

The RegenMed ecosystem and CHC concept utilize two distinct digital assets to perform its financial functions:

- **The Utility/Governance Token:** This coin is used by clinicians and MSOs for platform operations, credentialing, and participating in governance decisions. It aligns the professional interests of the medical community with the technological progress of

the platform.

- **The Stablecoin Dividend:** This is a dollar-pegged digital asset used for automated settlements with patients. When a researcher or other Circle Dataset licensee accesses a patient's data with explicit (smart contract) consent, the payment is executed instantly via a smart contract.

The GENIUS Act: Legalizing the Circle Coin

Signed into law on July 18, 2025, the GENIUS Act established the first comprehensive federal framework for stablecoin regulation in the United States. The Act defines "payment stablecoins" as digital assets pegged to a fiat currency (the U.S. dollar) and intended for use in payments and settlements. By providing clear federal guidelines, the GENIUS Act allows organizations like RegenMed to bypass the high fees and settlement delays of legacy payment processors in the context of CHCs.

Under the GENIUS Act, stablecoin issuers must maintain 100 percent reserve backing in liquid assets and provide monthly public disclosures. This regulatory clarity cements the U.S. Dollar's dominance in digital markets and ensures that "data dividends" represented by CHCs are treated as cash equivalents, not speculative securities. Large retail and healthcare entities are already integrating these stablecoin transaction rails to facilitate real-time, 24/7 commerce.

GENIUS Act Feature	Statutory Requirement	Impact on SSI
Reserve Backing	1:1 in cash or U.S. Treasuries.	Ensures the "Data Dividend" has real-world value.
Issuer Licensing	Approved by OCC, Fed, or State Regulators.	Creates a High-Trust financial environment.
Interchange Fees	Bypasses traditional card networks.	Maximizes the dividend reaching the patient.

Settlement Speed	Real-time, blockchain-based.	Enables instant payment upon data verification.

The impact of this automated settlement system can result in an approximate 70% reduction in the procurement costs of Real-World Evidence (RWE). By eliminating the administrative friction of manual recruitment and payment, researchers can access high-quality data at a fraction of the historical cost.

Regulatory Shielding—HTI-2, Information Blocking, and Valuation

For the modern healthcare executive, the SSI transition is not just a technology play; it is a mechanism for regulatory shielding and business valuation expansion. The Health Technology, Data and Interoperability Rules from the Office of the National Coordinator (ONC/ASTP) provide the legal framework for this shield.

HTI-2 Privacy Exceptions and Information Blocking

The HTI-2 Final Rule (2025/2026) expands the "Information Blocking" regulations to support the Trusted Exchange Framework and Common Agreement (TEFCA). While "information blocking" is generally prohibited, HTI-2 provides specific "privacy exceptions." These exceptions allow providers and technology developers to restrict data sharing unless it is mediated through secure, standards-based, and patient-authorized methods.

By adopting the RegenMed platform, hospital systems, MSOs, and other provider groups can leverage these exceptions to ensure that they are not "sharing" data in a way that creates liability, but are instead "facilitating" patient-mediated access. This provides a Liability Shield, as the organization is meeting the "manner exception" by fulfilling data requests in the manner the patient has authorized—through the SSI framework.

Increasing the Hospital System Valuation

Utilization by a hospital system, provider group or MSO of Circle Datasets – including the SSI structure -- creates a multiple expansion in business valuation. Traditional service-based MSOs, for example, are often valued at 6-8x EBITDA. By integrating the Circles Platform—becoming the co-owner of high-trust evidence and verified facts ready for review—the valuation multiple can expand to 12x -15x.

Pillar	Valuation Mechanic	Enterprise Impact
Payer Negotiation	Shift to high-margin contracts.	Prevents payment delays through proven results.
Liability Shield	Uses verified facts to lower insurance costs.	Blocks legal claims through Proven Medical Accuracy.
Federal Compliance	Automatic reporting via FHIR APIs.	Avoids financial penalties for info blocking.
Recruitment	Offers physicians control over their science.	Attracts top talent with new income streams.
Strategic Exit	Transition from "Service" to "Asset".	Multiple expansion from 6-8x to 12-15x.

The Cryptographic Kill Switch—Response to 2026 mandates

As of January 1, 2026, eighteen U.S. states have implemented comprehensive consumer data protection laws, including Indiana, Rhode Island, and Oregon. These laws grant consumers the "Right to Delete" their personal data, a mandate that presents an existential threat to traditional healthcare databases.

The Technical Challenge of the Right to Delete

In a legacy database, "deleting" a patient's information is a complex, manual, and often incomplete process. Fragments of patient data often remain in backups, audit logs, and secondary research datasets. Furthermore, if the data has been used to train an AI model, the "deletion" of the underlying data does not necessarily remove the patient's "influence" from the model's weights.

The Proposed Rule for Deletion Requests (e.g., the DROP platform in California) requires data brokers to execute deletion requests with a "reasonably high degree of certainty". For healthcare providers and MSOs, the failure to comply with these requests can lead to significant consumer harm and lawsuits related to Unfair or Deceptive Acts or Practices

(UDAP).

The RegenMed Kill Switch

The RegenMed response is the "cryptographic kill switch." Within the SSI framework, patient data is encrypted, and the decryption keys are controlled by the patient's identity wallet. When a patient exercises their "right to delete" or "revokes consent," the smart contract executes the kill switch, instantly and irrevocably destroying the decryption keys.

The encrypted data "blobs" may still exist in the storage layer, but they are technically and mathematically unreachable. This provides a "high-trust" guarantee of deletion that satisfies the 2026 mandates without requiring a complete rebuild of the database.

2026 Deletion Mandate	Statutory Requirement	Kill Switch Solution
Right to Deletion	Consumers can request deletion of all data.	Revocation of cryptographic decryption keys.
Opt-Out Propagation	Preferences must propagate to all downstream.	Smart contract terminates all active data licenses.
Audit Logs	Must maintain logs of detection/enforcement.	Blockchain ledger provides a permanent audit trail.
Verification Guardrails	Must verify identity before deletion.	SSI identity wallet provides 100% verification.

OPERATIONALIZING

Proven Medical Accuracy—USCDI Baselines

The shift toward the 2026 Veracity Mandate is operationalized through the USCDI standards. USCDI defines the baseline of data elements that must be available for interoperable exchange.

The Evolution of USCDI (v4 through v6)

In 2024 and 2025, the ONC (now ASTP) raised the baseline for certified health IT and adopted USCDI v3 as the new baseline as of January 1, 2026. The forward-looking organization must adhere to USCDI v5 and v6 to meet the veracity requirements of 2026.

- **USCDI v5 (Released July 18, 2024):** Introduced "Observations," "Clinical Notes", and "Provenance." Provenance is critical for Proven Medical Accuracy, as it establishes the authenticity, reliability, and trustworthiness of the data content.
- **USCDI v6 (Released July 24, 2025):** Added "Facility Address", "Care Plan", and "Family Health History." The inclusion of the Care Plan data element allows for the exchange of patient goals and strategies, moving the data model from "episode-centric" to "longitudinal".

Designing for Proven Results

By "Designing for Proven Results"—defining clinical rules and USCDI standards *before* the patient visit—the MSO ensures that every data point captured is a "Verified Fact Ready for Review." This protocol-driven capture eliminates the post-hoc cleanup and "data wrangling" that currently consumes 80% of research budgets.

The implementation of USCDI v6 elements like the "Portable Medical Order" (e.g., DNR/Comfort measures) ensures that clinical decisions are made based on high-trust evidence that reflects the patient's current state and preferences, directly impacting quality scores and payer incentives.

The Veracity Mandate and Algorithm Transparency

A final critical component of the 2026 regulatory environment is the "Algorithm Transparency Rule".

Algorithm Transparency (Predictive DSI)

HTI-1 established first-of-their-kind transparency requirements for AI and predictive algorithms used in certified health IT. Developers must now provide "Source Attributes" for these Decision Support Interventions (DSI). Clinicians must have access to information regarding the algorithm's development, including the training data's demographics and the

"FAVES" criteria (Fair, Appropriate, Valid, Effective, Safe).

For the healthcare executive, this means that the "black box" AI of the past is no longer compliant. Algorithms must be supported by the High-Trust Evidence of the clinical data they process. Organizations using the RegenMed SSI model are uniquely positioned to meet these requirements because their data is already captured under the protocol-driven standards of the 2026 Veracity Mandate.

The Insights Condition

The "Insights Condition" of certification (finalized in HTI-1) requires health IT developers to report metrics on how their technology is used in support of care delivery. This includes reporting on the pre-processing of clinical documents (C-CDA) and the volume of data requests made via FHIR APIs. This data is made publicly available by the ONC, providing a transparent look at which vendors and providers are truly participating in the interoperable ecosystem, and which are lagging behind.

CONCLUSION

The evidence is dispassionate and definitive: the era of Data Custodianship by hospital systems, other provider groups, and MSOs is over. Organizations that attempt to maintain legacy data silos or rely on the myth of anonymity are exposing themselves to catastrophic regulatory and financial risk. The transition to Self-Sovereign Health Identity is the only pathway that secures a definitive liability shield as well as a higher business valuation from 2026 forward.

Executive Recommendations For Provider Groups and MSOs

- **Acknowledge the Mosaic Effect:** Cease the sale of "de-identified" data under Safe Harbor protocols. The technical reality of linkage attacks renders these datasets identifiable, creating a long-term liability.
- **Transition to the Split-IP Model:** Formalize contractual relationships where the practice owns the raw data, the platform owns the AI weights, and the patient owns the sovereignty and dividends. This eliminates "unjust enrichment" and aligns interests for longitudinal data capture.

- **Implement the GENIUS Act Settlement Rail:** Integrate stablecoin settlements for Circle Health Coins ("data dividends") to reduce RWE procurement costs substantially. Automate the payout process via smart contracts to ensure real-time participation incentives for patients.
- **Operationalize USCDI v6:** Ensure that all clinical workflows are designed to capture USCDI v5 and v6 elements—specifically Provenance and Care Plans—to meet the 2026 veracity mandate for proven medical accuracy.
- **Deploy the Cryptographic Kill Switch:** Respond to 2026 "right to delete" mandates with a technical solution that revokes decryption keys, providing a high-trust guarantee of data revocation.

By moving from a model of patient data brokerage to one of sovereignty, the healthcare industry can finally deliver on the promise of the 21st Century Cures Act: a digital ecosystem where patients are empowered, clinicians are protected, and clinical truth is the ultimate asset.

REFERENCES

45 CFR 164.524 -- Access of individuals to protected health information. - eCFR. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.524

45 CFR § 164.524 - Access of individuals to protected health information., https://www.law.cornell.edu/cfr/text/45/164.524

HIPAA and the Right of Access: OCR's Heightened Enforcement - Coates' Canons. https://canons.sog.unc.edu/blog/2023/02/10/hipaa-and-the-right-of-access-ocrs-heightened-enforcement/

When the Rules Changed: The Top 2025 Privacy and Security https://www.healthcarelawinsights.com/2026/02/when-the-rules-changed-the-top-2025-privacy-and-security-issues-still-shaping-healthcare/

Medical Record Retrieval Costs by State (2025 Update) - Tavrn. https://www.tavrn.ai/blog/medical-record-retrieval-costs

The need for clear medical data ownership laws - PMC. https://pmc.ncbi.nlm.nih.gov/articles/PMC12763853/

Medical Record Laws by State: Key Statute Types for Compliance | ChartRequest. https://www.chartrequest.com/articles/medical-record-laws-by-state

HTI-2 Final Rule - ASTP - Assistant Secretary for Technology Policy. https://healthit.gov/regulations/hti-rules/hti-2-final-rule/

Health Law Highlights - Healthcare Empowered. https://texashealthlaw.com/category/health-law-highlights/

Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons - Federal Register. https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern

Mosaic effect - Wikipedia. https://en.wikipedia.org/wiki/Mosaic_effect

Responsible data sharing: Identifying and remedying possible re-identification of human participants ResearchGate. https://www.researchgate.net/publication/374205670_Responsible_data_sharing_Identifying_and_remedying_possible_re-identification_of_human_participants

Enabling realistic health data re-identification risk assessment through adversarial modeling.

https://www.researchgate.net/publication/348752127_Enabling_realistic_health_data_re-identification_risk_assessment_through_adversarial_modeling

(PDF) A Framework for Efficient Data Anonymization under Privacy and Accuracy Constraints – ResearchGate .https://www.researchgate.net/publication/48205508_A_Framework_for_Efficient_Data_Anonymization_under_Privacy_and_Accuracy_Constraints

Beyond Refusal: Probing the Limits of Agentic Self-Correction for Semantic Sensitive Information - arXiv.org .https://arxiv.org/html/2602.21496v1

Autoencoder-Enhanced Hierarchical Mondrian Anonymization via Latent Representations - Preprints.org. https://www.preprints.org/manuscript/202602.0124/v1/download

https://www.researchgate.net/publication/400117945_Data_Governance_Strategies_for_Mitigating_Privacy_Risks_in_Automated_Learning_Systems

Privacy-Preserving Pangenome Graphs - bioRxiv. https://www.biorxiv.org/content/10.64898/2026.02.16.706152v1.full-text

NIH Controlled-Access Data Policy and Proposed Revisions to NIH Genomic Data Sharing Policy - Federal Register https://www.federalregister.gov/documents/2025/12/18/2025-23246/nih-controlled-access-data-policy-and-proposed-revisions-to-nih-genomic-data-sharing-policy

13 J Barbara J. Evans, Ph.D., J.D., LL.M.* Abstract Since 2003, U.S. federal funders' scientific data sharing p – SSRN https://papers.ssrn.com/sol3/Delivery.cfm/6110307.pdf?abstractid=6110307&mirid=1&type=2

De-identifying Data in Clinical Trials. https://www.appliedclinicaltrialsonline.com/view/de-identifying-data-clinical-trials

De-Identified and Unregulated: How Data Brokers Outpace State Privacy Laws. https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1674&context=jetlaw

The Basics: Stablecoins and The GENIUS Act | Winthrop ... - JD Supra. https://www.jdsupra.com/legalnews/the-basics-stablecoins-and-the-genius-3747119/

GENIUS Act and a New Digital Asset Era - Law Offices of Snell ....https://www.swlaw.com/publication/genius-act-and-a-new-digital-asset-era/

How 2025 Transformed Digital Assets: What Leaders Need to Know for 2026. https://www.gfrlaw.com/what-we-do/insights/how-2025-transformed-digital-assets-what-leaders-need-know-2026

Stablecoins: Issues for regulators as they implement GENIUS Act - Brookings.

https://www.brookings.edu/articles/stablecoins-issues-for-regulators-as-they-implement-genius-act/

CHIME Responds to CMS & ASTP/ONC's RFI on the Health Technology Ecosystem. https://chimecentral.org/resource-post/chime-responds-to-cms-astponc-rfi-on-health-technology-ecosystem

Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions to Unleash Prosperity - Regulations.gov. https://www.regulations.gov/document/HHS-ONC-2025-0005-0001

Indiana and Rhode Island Complete the 2026 State Privacy Trinity: What Businesses Need to Know About America's Newest Data Protection Laws - Compliance Hub Wiki .https://www.compliancehub.wiki/indiana-and-rhode-island-complete-the-2026-state-privacy-trinity-what-businesses-need-to-know-about-americas-newest-data-protection-laws/

Delete Request and Opt–out Platform ("DROP") System Requirements Part 1. https://cppa.ca.gov/regulations/pdf/drop_written_comments.pdf

HTI-1 Final Rule - ASTP - Assistant Secretary for Technology Policy – ONC .https://healthit.gov/regulations/hti-rules/hti-1-final-rule/

ONC Standards Bulletin 2024-2 - ASTP - Assistant Secretary for Technology Policy. https://healthit.gov/standards-and-technology/onc-standards-bulletin/onc-standards-bulletin-2024-2/

USCDI Data Element - HealthIT.gov. https://www.healthit.gov/isp/taxonomy/term/3276/uscdi-v5

ONC Standards Bulletin 2025-2 - ASTP - Assistant Secretary for Technology Policy. https://healthit.gov/standards-and-technology/onc-standards-bulletin/onc-standards-bulletin-2025-2/

ONC Standards Bulletin 2025-1 - ASTP - Assistant Secretary for Technology Policy .https://healthit.gov/standards-and-technology/onc-standards-bulletin/onc-standards-bulletin-2025-1/

ONC Standards Bulletin - ASTP - Assistant Secretary for Technology Policy - HealthIT.gov. https://healthit.gov/standards-and-technology/onc-standards-bulletin/

The Office of the National Coordinator for Health Information Technology (ONC) Announces Special Emphasis Notice (SEN) Interest. https://healthit.gov/wp-content/uploads/2024/05/LEAP-FY2024-SEN_508.pdf

Health Data, Technology, and Interoperability ... - Federal Register. https://www.federalregister.gov/documents/2024/01/09/2023-28857/health-data-technology-and-

interoperability-certification-program-updates-algorithm-transparency-and

2024 Report to Congress - HealthIT.gov. https://healthit.gov/wp-content/uploads/2024/09/2024-Cures-Act_RTC_PPT_508.pdf