PROGRAM MATERIALS
Program #36101
April 16, 2026

Reinventing Project Financing Using Real World Asset (RWA) Tokenization on the Blockchain

- Charles R. Macedo, Of Counsel - Amster, Rothstein & Ebenstein LLP

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

National Security & Data Privacy: Complying with the Bulk Data Rule and the New Data Security Program

Charles R. Macedo

April 16, 2026

DISCLAIMER

The following presentation reflects the opinion of its human author and does not necessarily represent the views of his respective clients, partners, employers, or of Amster, Rothstein & Ebenstein LLP, nor Celesq or any of its officers, or employees.

Additionally, the following content is presented solely for the purposes of discussion and illustration and does not comprise, nor is to be considered, as legal or business advice.

No humans were hurt in making this presentation, but AI assisted in its preparation.

About our Speakers

Charles R. Macedo is a seasoned intellectual property attorney with deep expertise at the intersection of emerging technologies, data-driven businesses, and commercialization. He is recognized as an author, thought leader and frequent lecturer in intellectual property, blockchain, artificial intelligence/software, and data monetization. With a technical background in physics and decades of experience guiding Unicorns, startups, financial services firms, and technology innovators, he has developed IP strategies as they launch and monetize new product lines resulting in collections of hundreds of millions of dollars of royalty revenue.

J.D. 1989, Columbia Law School; B.S./M.S., Physics, 1986; former Law Clerk to Hon. Daniel M. Friedman at U.S. Court of Appeals for the Federal Circuit.

Agenda

1. **Origins of the Bulk Data Rule:**
   - Executive Order 14117 and the Data Security Program
2. **Defining the Regulatory Scope:**
   - Countries of Concern, Covered Person and Data Transactions
3. **Data Types and Bulk Thresholds:**
   - Understanding the Regulated Data Categories
4. **Prohibited v. Restricted Transactions:**
   - Understanding Transaction Classifications and Their Impact
5. **Enforcement and Penalties:**
   - Consequences of Non-Compliance
6. **Additional State Statutes:**
   - Texas, Montana, Florida
7. **Compliance Strategy:**
   - Strategic Steps for Institutions

1 Origins of the Bulk Data Rule:

- **Executive Order 14117**
- **The Data Security Program**

The National Security Threat

The Core Threat

Countries of concern exploit bulk sensitive personal data to threaten U.S. national security through multiple vectors including AI-driven surveillance, economic espionage, cyber-enabled activities, and the development of advanced technologies for military and intelligence purposes. Even anonymized data presents significant risks when aggregated and analyzed at scale.

Malicious Activities Enabled by Data Access

Foreign adversaries leverage bulk personal data for surveillance operations targeting journalists, political figures, and marginalized communities; blackmail and coercion of government officials and defense contractors; tracking military and intelligence personnel; curbing dissent by U.S. persons; and conducting foreign malign influence campaigns that undermine democratic institutions.

Healthcare Data Vulnerability

Hospitals and academic research institutions are prime targets because health data reveals exploitable personal information including medical conditions, genetic predispositions, mental health status, and demographic patterns. Genomic data is especially valuable for developing biotechnologies, personalized bioweapons, and advancing AI systems trained on human biological patterns.

Key Threat Vectors

AI Development

Training AI on sensitive U.S. data for military applications and surveillance technologies

Biotech Advancement

Exploiting genomic data for biological weapons development and genetic surveillance

Mass Surveillance

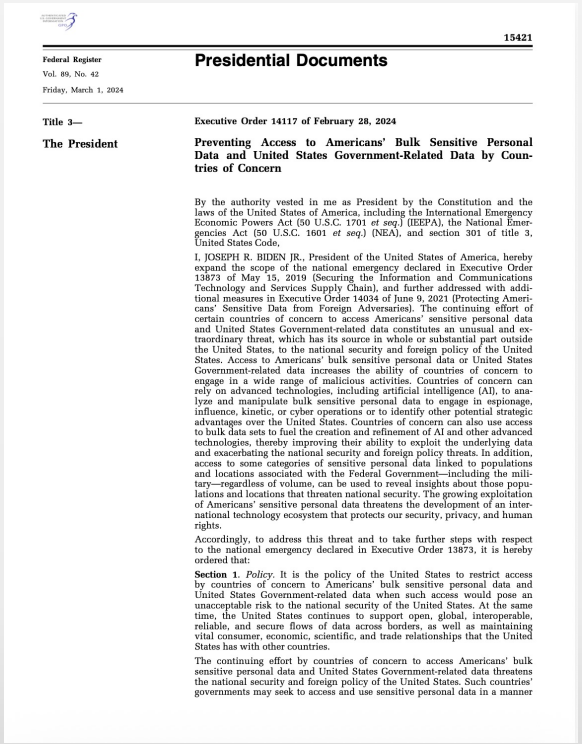
Aggregating data to track populations, predict behaviors, and identify vulnerabilities

Economic Espionage

Stealing research, trade secrets, and intellectual property from U.S. institutions

Executive Order 14117, 89 Fed. Reg. 15421, signed Feb. 24, 2024, by President Biden

"Preventing Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern"



15421

Federal Register
Vol. 89, No. 42
Friday, March 1, 2024

Presidential Documents

Title 3—
The President

Executive Order 14117 of February 28, 2024

Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), and section 301 of title 3, United States Code,

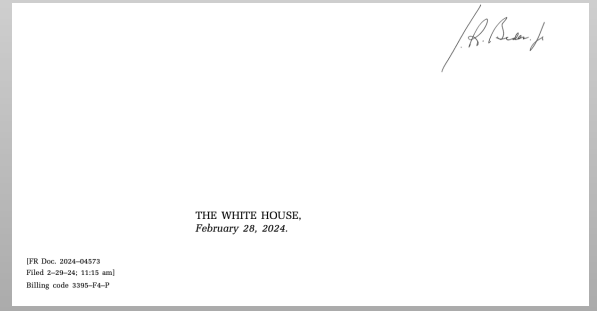
I, JOSEPH R. BIDEN JR., President of the United States of America, hereby expand the scope of the national emergency declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and further addressed with additional measures in Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries). The continuing effort of certain countries of concern to access Americans' sensitive personal data and United States Government-related data constitutes an unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security and foreign policy of the United States. Access to Americans' bulk sensitive personal data or United States Government-related data increases the ability of countries of concern to engage in a wide range of malicious activities. Countries of concern can rely on advanced technologies, including artificial intelligence (AI), to analyze and manipulate bulk sensitive personal data to engage in espionage, influence, kinetic, or cyber operations or to identify other potential strategic advantages over the United States. Countries of concern can also use access to bulk data sets to fuel the creation and refinement of AI and other advanced technologies, thereby improving their ability to exploit the underlying data and exacerbating the national security and foreign policy threats. In addition, access to some categories of sensitive personal data linked to populations and locations associated with the Federal Government—including the military—regardless of volume, can be used to reveal insights about those populations and locations that threaten national security. The growing exploitation of Americans' sensitive personal data threatens the development of an international technology ecosystem that protects our security, privacy, and human rights.

Accordingly, to address this threat and to take further steps with respect to the national emergency declared in Executive Order 13873, it is hereby ordered that:

Section 1. *Policy.* It is the policy of the United States to restrict access by countries of concern to Americans' bulk sensitive personal data and United States Government-related data when such access would pose an unacceptable risk to the national security of the United States. At the same time, the United States continues to support open, global, interoperable, reliable, and secure flows of data across borders, as well as maintaining vital consumer, economic, scientific, and trade relationships that the United States has with other countries.

The continuing effort by countries of concern to access Americans' bulk sensitive personal data and United States Government-related data threatens the national security and foreign policy of the United States. Such countries' governments may seek to access and use sensitive personal data in a manner

Signed February 28, 2024, by President Biden



THE WHITE HOUSE,
February 28, 2024.

[FR Doc. 2024-04573
Filed 2-29-24; 11:15 am]
Billing code 3395-F4-P

Executive Order 14117: Policy Framework

Core Policy Objectives

- **Protect National Security:** Restrict access by countries of concern to sensitive data when it poses unacceptable risks
- **Maintain Open Internet:** Support secure, global, interoperable data flows for legitimate commerce and research
- **Preserve Scientific Collaboration:** Protect ongoing international research partnerships and innovation
- **Enable Trade Relationships:** Avoid broad decoupling while addressing specific security threats

What the Order Does NOT Do

The Executive Order explicitly does NOT impose generalized data localization requirements, broadly prohibit commercial transactions, or undermine public access to taxpayer-funded research results, patient data access, or health information interoperability.

Strategic Approach

1. **Targeted Restrictions**
   Carefully calibrated actions addressing specific national security threats.
2. **Risk-Based Framework**
   Volume thresholds based on data type vulnerability to exploitation.
3. **Transaction-Specific**
   Focus on data brokerage, vendor, employment and investment agreement.
4. **Security Requirements**
   CISA-developed cybersecurity standards for restricted transactions

Presidential Declaration

"The United States has long recognized the vital importance of maintaining open, global, interoperable, reliable, and secure flows of data across borders... However, the growing exploitation of Americans' sensitive personal data by countries of concern threatens our national security, foreign policy, and economy ."

Implementation Timeline

Critical dates for institutions to achieve compliance

2025

April 8, 2025
Rule Effective Date

Majority of the Data Security Program took effect. All covered entities required to comply with prohibited transaction restrictions and make good faith efforts to comply with restricted transaction requirements.

- Most prohibitions and restrictions became enforceable

July 8, 2025
Enforcement Begins

The 90-day enforcement grace period concluded. DOJ commenced full enforcement with civil and criminal penalties applicable. Good faith compliance efforts no longer sufficient—entities must be in full compliance.

- DOJ may pursue enforcement for any violations

October 6, 2025
Full Compliance Due

All compliance obligations must be implemented. Includes CISA security requirements, data compliance programs, annual audits, due diligence procedures, and recordkeeping systems for restricted transactions.

- Complete compliance framework required

Current Status: Immediate Action Required

Institutions are now operating in an environment where all prohibited and restricted transactions are subject to enforcement . Institutions must have already implemented compliance measures or face significant penalties.

Immediate Risks

- Vendor agreements with overseas providers
- International research collaborations
- Cloud services with foreign infrastructure

Required Actions Now

- Conduct comprehensive data mapping
- Screen all vendors and partners
- Implement security controls

2 Defining the Regulatory Scope:

- Countries of Concern
- Covered Person
- Data Transactions

Countries of concern § 206.601

Designated based on demonstrated intent and capability to exploit U.S. sensitive data

Impact on Institutions

Companies and institutions should **immediately assess all international relationships**, vendor agreements, research collaborations, and data processing activities for connections to these six countries.

China (including Hong Kong and Macau) (NOT Taiwan)

Cuba

Iran

North Korea

Russia

Venezuela

Designation Criteria

Countries were designated based on both intent and capability to exploit bulk U.S. sensitive personal data to harm national security through espionage, surveillance, coercion, and cyber-enabled activities.

Intent Factors

- Demonstrated pattern of data exploitation
- Active malign influence operations
- Use of data for coercion and blackmail

Capability Elements

- Advanced cyber operations infrastructure
- AI and data analytics capabilities
- Access to global technology supply chains

Dynamic Designation

The Attorney General, in coordination with other agencies, may add or remove countries of concern as threats evolve. Institutions should monitor for updates to ensure ongoing compliance with changing geographic scope.

Who are "Covered Persons"? § 202.211

Entity-Based Criteria:

- **Organizational Ties**
  - Any entity **organized under the laws of a country of concern** or with its principal place of business in these countries.
- **Ownership Threshold**
  - Entities 50% or more owned directly or indirectly, by a country of concern or another covered person – including through complex multi-layer ownership structures
- **Employment Relationship**
  - Foreign employees or contractors of countries of concern or covered entity employers.

Individual-Based Criteria

- **Residency Requirement**
  - Foreign individuals primarily residents of countries of concern, regardless of citizenship or employment status
- **DOJ Designation**
  - Any person specifically designated by the Attorney General based on national security concern published in the **Covered Person List**

Practical Examples of “Covered Persons”

Vendor Scenario

- A cloud service provider incorporated in Cayman Islands but majority-owned by Chinese investors = **Covered Person**

Employment Scenario

- A data analyst working for your hospital from Iran via remote access = **Covered Person**

Investment Scenario

- A Cuban based venture capital fund investing in your technology subsidiary = **Covered Person**

Research Scenario

- A contract research organization in China processing clinical trial samples = **Covered Person**

Due Diligence “Best” Practices for “Covered Persons”

Companies and Institutions should continuously screen all counterparties including:

- ❑ Employees
- ❑ Contractors
- ❑ Investors
- ❑ Research Partners

Using **DOJ’s Covered Person List** is a minimum but not sufficient requirement:

- ✓ Organizations should conduct independent ownership analysis assessment.

Covered Data Transactions

Critical Requirement: Access Trigger

A transaction becomes a "**covered data transaction**" only if it provides a country of concern or covered person with "**access**" to **bulk sensitive personal data** or **government-related data**.

"**Access**" includes the **ability** to:

- view
- process
- store
- analyze
- transfer

Covered Data Transactions § 202.210

Categories of Regulated Data Transactions under Data Security Programs

Data Brokerage § 202.214

Definition: Selling, licensing, renting, trading, transferring, releasing, disclosing, or providing access to data where the recipient did not collect the data directly from the individuals.

Employment Agreements § 202.217

Definition: Workforce arrangements where an individual works or performs job functions directly for a person in exchange for compensation, including board, executive, or operational roles

Vendor Agreements § 202.258

Definition: Arrangements where an entity provides goods or services to another for payment or consideration, including IT services, cloud storage, analytics, and processing.

Investment Agreements § 202.228

Definition: Agreements where a person obtains direct or indirect ownership rights in U.S. real estate or a U.S. legal entity, with exceptions for passive investments.

3 Data Types and Bulk Thresholds:

- **Understanding the Regulated Data Categories**

Bulk Thresholds § 202.205
(When Data Becomes Regulated)

Threshold Calculation Methodology

Rolling 12-Month Period

Calculated by aggregating all transactions within the preceding 12 months, whether in a single transaction or accumulated over time

Aggregation Requirement

Multiple transactions involving the same U.S. person and same covered person are aggregated toward threshold calculation

Combined Data Rule

Datasets containing multiple data categories are subject to the **lowest applicable threshold** for any category present

Complete Threshold Matrix

Most sensitive (lowest threshold) ← → Least sensitive (highest threshold)

100 U.S. Persons	1000 U.S. Persons	10,000 U.S. Persons	100,000 U.S. Persons
Human genomic data	Biometric identifier	Personal health data	Covered personal identifiers
	Precise geolocation	Personal financial data	
	Other Human 'omic data		

Lowest relevant threshold applies to any given data set

Categories of Sensitive Personal Data §202.249

(Restricted regardless of anonymization, pseudonymization, or encryption)

Covered Personal Identifiers
§ 202.212

- Identifiers **linked** to another identifier
  - Social Security Numbers
  - Driver's license numbers
  - Financial account numbers
  - Device identifiers and IP addresses

Precise Geolocation Data
§ 202.242

- Location data accurate within **1,000 meters or less**
  - GPS coordinates
  - Wi-Fi positioning data
  - Cell tower triangulation
  - Mobile Application tracking

Biometric Identifiers
§ 202.204

- **Measurable** physical or behavioral characteristics
  - Facial image and scans
  - Fingerprints and palm prints
  - Retina and iris scans
  - Voice prints and gait patterns

Human 'Omic Data
§ 202.224

- Systems-level analysis of human biological molecules
  - **Genomics:** Nucleic acid sequences
  - **Epigenomics**: Gene expression modifications
  - **Proteomic:** Protein expression analysis
  - **Transcriptomic**: RNA transcript analysis

Personal Health Data
§ 202.241

- Information relation to an individual's health condition
  - Medical diagnoses and treatment
  - Prescription records
  - Mental health conditions
  - Genetic test results

Personal Financial Data
§ 202.241

- Information about financial accounts and transactions
  - Credit card transactions
  - Bank account information
  - Credit histories and scores
  - Investment Portfolio data

4 Prohibited v. Restricted Transactions

- **Understanding Transaction Classifications and Their Impact**

Prohibited Transactions
(No compliance network can authorize these transactions)

Prohibition #1: Data Brokerage § 202.301

Any data brokerage transaction involving bulk sensitive personal data or government-related data with a covered person or country of concern is prohibited.

What is Data Brokerage?

Selling, licensing, renting, or providing data where the recipient did not collect it directly from individuals.

Healthcare Examples:

- Licensing de-identified patient data to a Chinese company
- Selling genomic datasets to a Russian research institute

Prohibition #2: Human 'Omic or Biospecimen Data § 202.303

Any transaction providing a covered person or country of concern with access to bulk human 'omic data or biospecimens is absolutely prohibited.

Scope of Prohibition

- **Genomic Data:** Whole genome, exome, gene panels
- **Biospecimens:** Blood, tissue, saliva from which 'omic data could be derived
- **Other 'Omics:** Epigenomic, proteomic, transcriptomic data

Prohibited transactions are prohibited unless covered by a specific or general license § 202.801 - 802

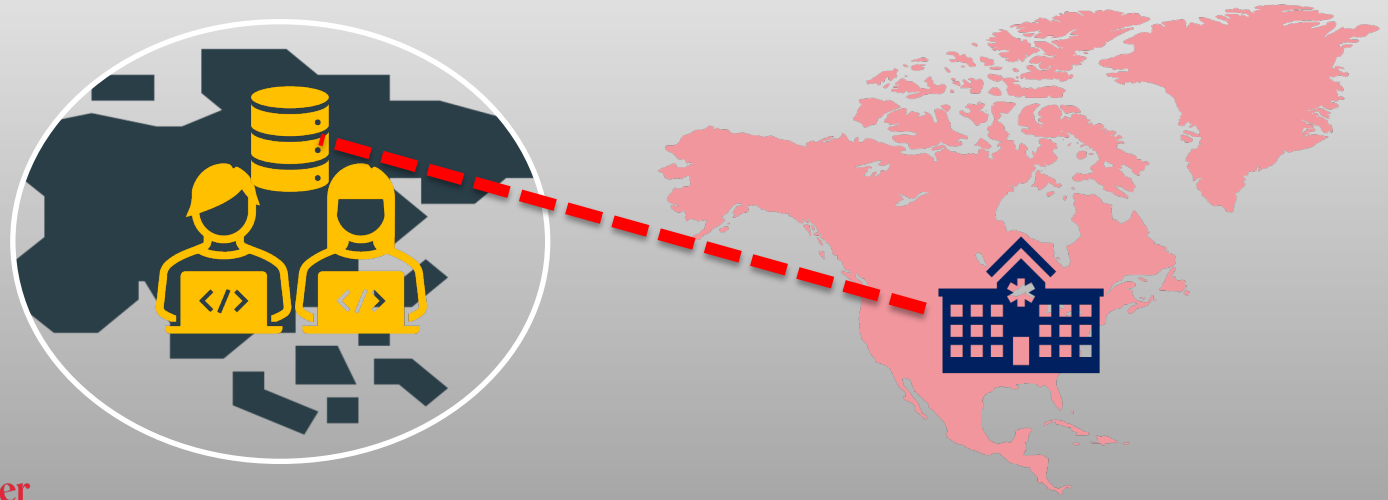
Unlike restricted transactions, no compliance framework, or security controls can authorize these transactions. Institutions should identify and terminate any existing prohibited arrangements immediately to avoid severe penalties.

Real-World Examples

How the Bulk Data Rule affects common hospital and research activities

Scenario 1: AI Health Driven Chatbot

A U.S. entity licenses an AI health driven chatbot trained on bulk U.S. sensitive personal data to a Shanghai entity, where it knows or should know the chatbot can be used to reproduce or disclose content or analysis of the underlying training data.



Analysis

Type of Transaction:

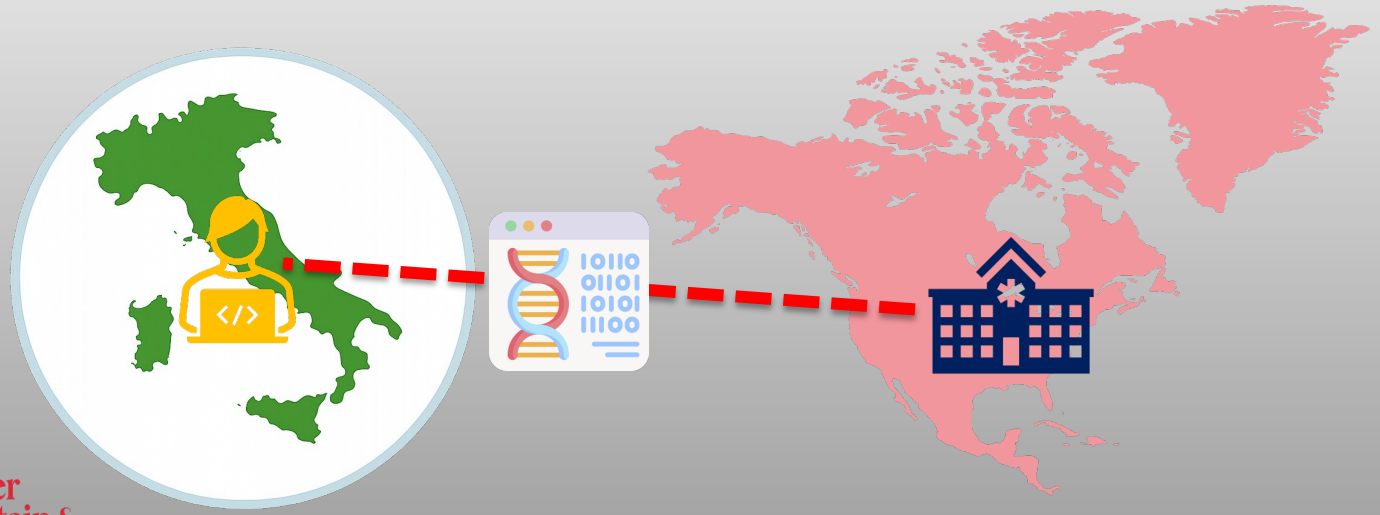
Prohibited Transaction
(data-brokerage transaction)

Real-World Examples

How the Bulk Data Rule affects common hospital and research activities

Scenario 2: Contractual Provisions

A U.S. business sells bulk U.S. human genomic data to **Italy,** a non-covered foreign entity, **without contractual restrictions** preventing resale or data brokerage to a country of concern or a covered person.



Analysis

Type of Transaction:

Prohibited Transaction
(Onward Transfer – Data Brokerage)

Requirements:

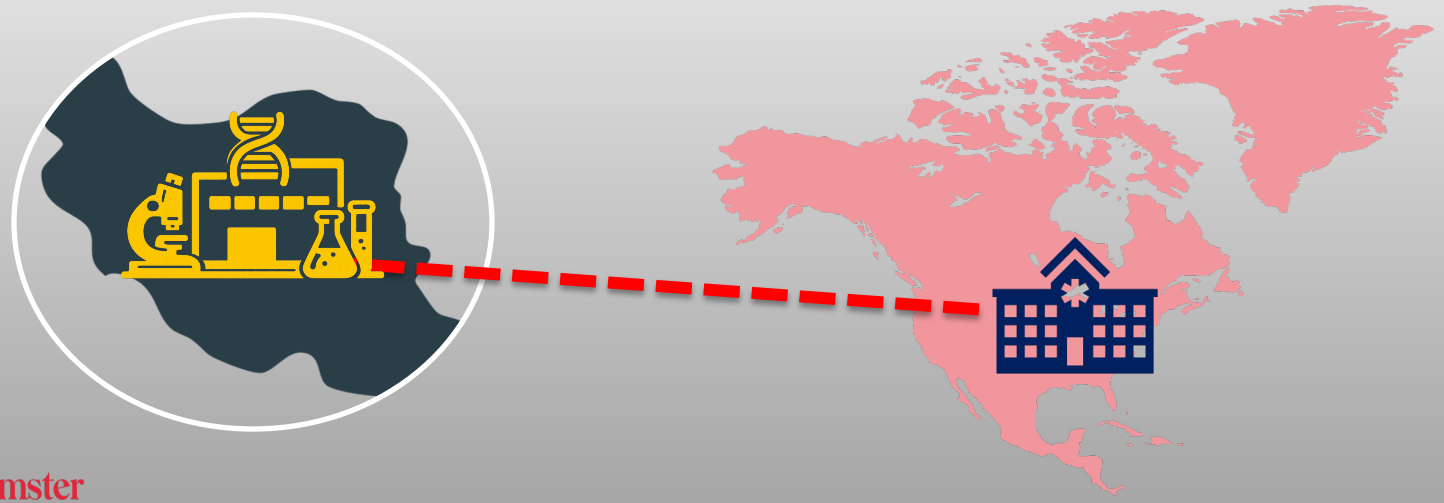
Any data brokerage transaction with a foreign entity should include contractual provisions preventing the foreign entity from engaging in a covered transaction. § 202.302

Real-World Examples

How the Bulk Data Rule affects common hospital and research activities

Scenario 3: Biospecimen

A **U.S. cancer center's** proposal to send 200 tumor samples of **U.S. persons** to an Iranian genomics lab for sequencing is a prohibited transaction.



Analysis

Type of Transaction:

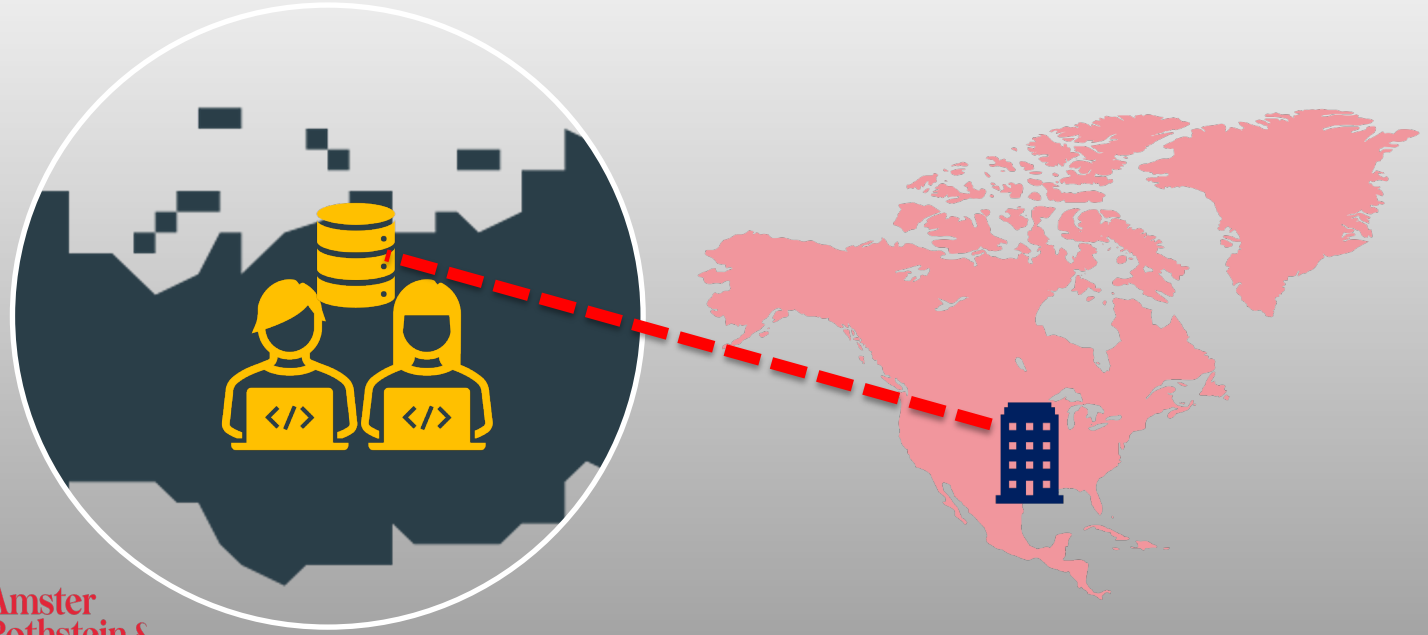
Prohibited Transaction
(Biospecimen from which bulk human `omic data could be derived)

Real-World Examples

How the Bulk Data Rule affects common hospital and research activities

Scenario 4: Data license

A **biobank's plan** to license de-identified **U.S.** genomic data from 5,000 participants to a Russian biotech firm.



Analysis

Type of Transaction:

Prohibited Transaction (Human 'Omic)

Restricted Transactions: Conditional Access § 202.401

Permitted only if comprehensive cybersecurity and compliance requirements are met

Key Distinction

Restricted transactions are **not prohibited** but require implementing specific security and compliance measures. Organizations should weigh the benefits against the significant compliance overhead.

Vendor Agreements

- Cloud services, IT support, analytics, CRO services

Employment Agreements

- Remote employees, contractors, consultants with data access.

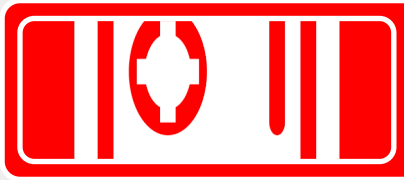
Investment Agreements

- Foreign investment in entities with data access.

Restricted Transactions: Conditional Access

Permitted only if comprehensive cybersecurity and compliance requirements are met

Mandatory Requirements for Restricted Transactions

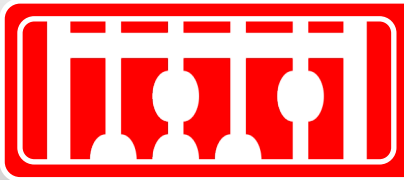


CISA Security Requirement

- Implement cybersecurity framework with asset management, access controls, vulnerability remediation, MFA, encryption, and auditing.

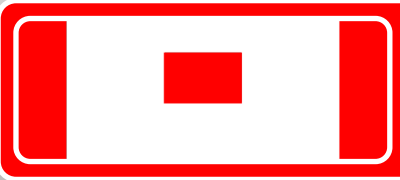
Data Compliance Program

- Establish written, risk-based procedures for data flows and vendor verification, with annual certification.



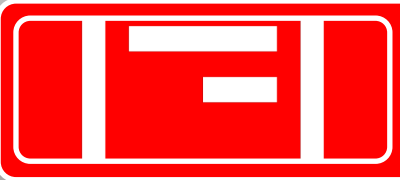
Annual Independent Audits

- Conduct annual audits by a qualified, independent auditor who is not a covered person, with reports to senior officers.



10-Year Recordkeeping

- Maintain detailed records of all restricted transactions for at least 10 years in an auditable manner.



Contractual Prohibitions & Onward Transfer Safeguards

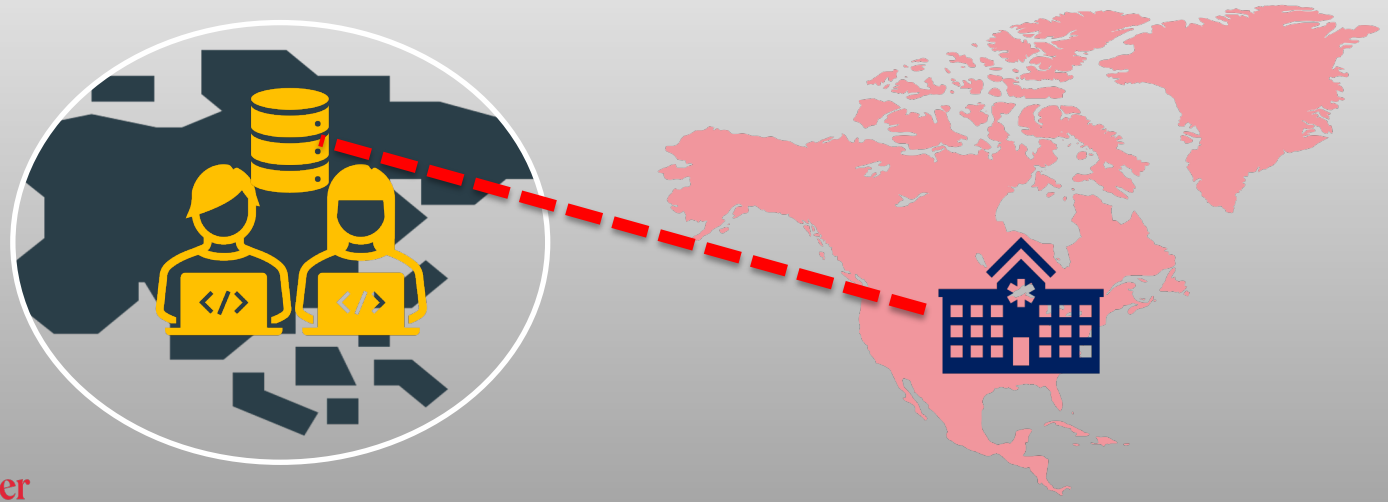
- Include clauses prohibiting resale or transfer of data to covered persons.

Real-World Examples

How the Bulk Data Rule affects common hospital and research activities

Scenario 1: Cloud Services with Overseas Infrastructure

A **hospital** uses a major cloud provider for personal health data hosting. The provider has **data centers** worldwide, including in **China**, and **Chinese employees** can access bulk data for technical support.



Analysis

Type of Transaction:

Restricted Transaction
(Vendor Agreement)

Requirements:

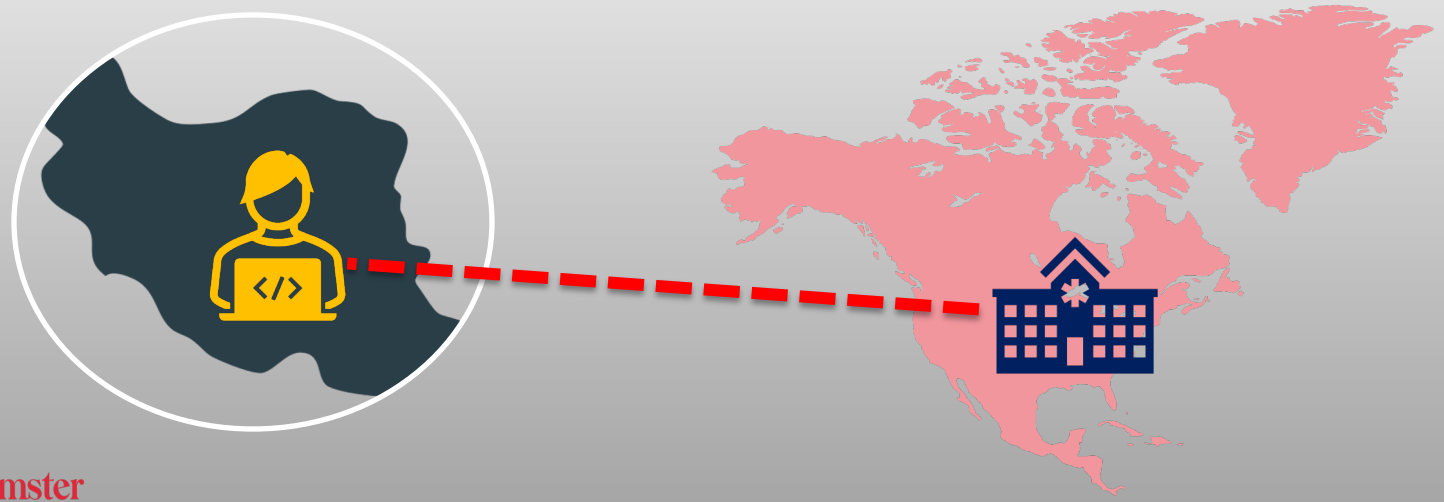
- CISA security controls
- Data Compliance Program
- Audit
- 10-year records
- Contractual

Real-World Examples

How the Bulk Data Rule affects common hospital and research activities

Scenario 2: Employees in Countries of Concern

A **hospital system** hires a data scientist living in Iran as an independent contractor to analyze patient outcomes (not including human 'omic data or human biospecimen) for quality improvement.



Analysis

Type of Transaction:

Restricted Transaction (Employment)

Requirements:

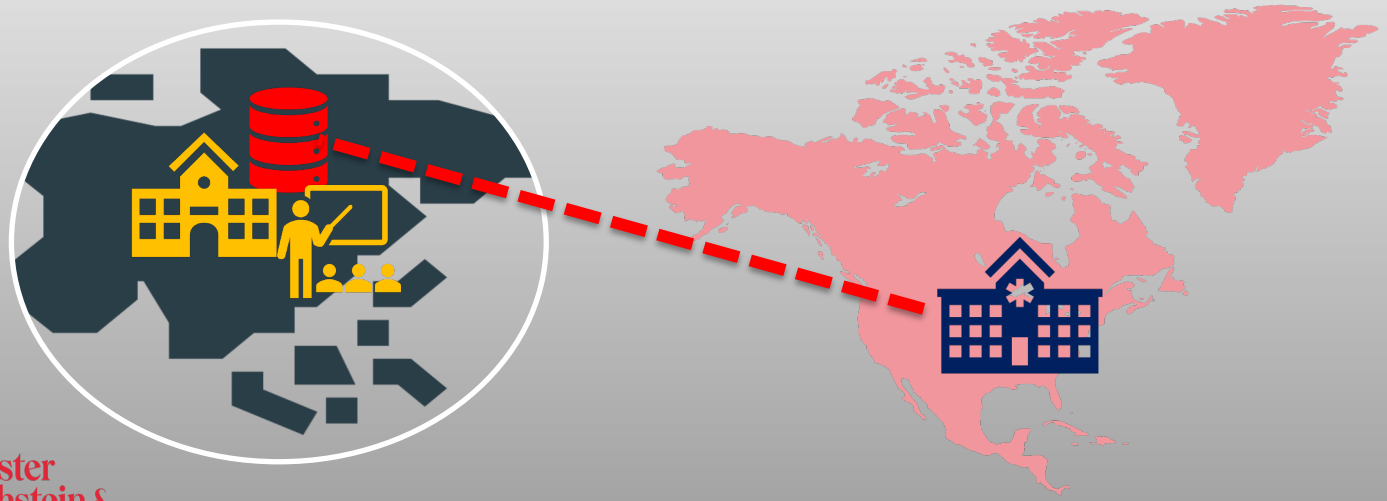
- CISA security controls
- Data Compliance Program
- Audit
- 10-year records
- Contractual

Real-World Examples

How the Bulk Data Rule affects common hospital and research activities

Scenario 3: International Research Collaboration

An **AMC** is partnering with a Chinese university on a cardiovascular study. They plan to share de-identified patient health data (not including human 'omic data or human biospecimen) from 15,000 U.S. participants.



Analysis

Type of Transaction:

Restricted Transaction
(Vendor Agreement)

Requirements:

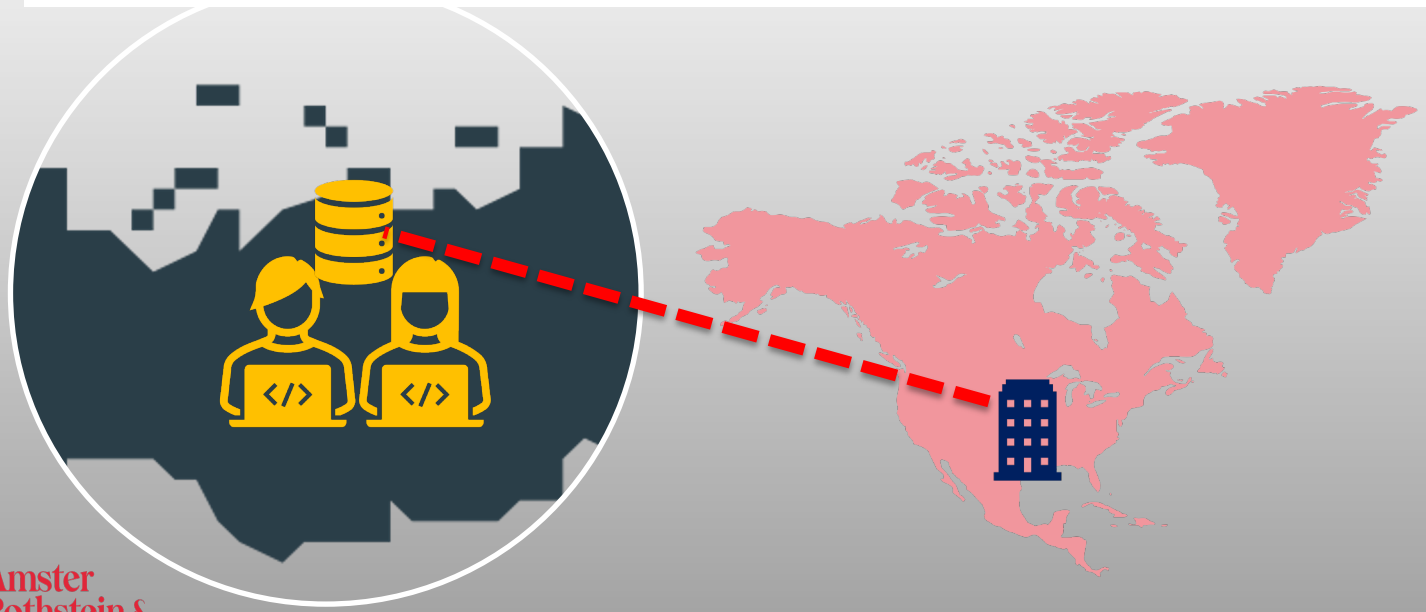
- CISA security controls
- Data Compliance Program
- Audit
- 10-year records
- Contractual

Real-World Examples

How the Bulk Data Rule affects common hospital and research activities

Scenario 4: Contract Research Organization

A **U.S. pharma company** hires a Russian CRO for a multi-site trial. The CRO needs access to de-identified health data (not including human 'omic data or human biospecimen) from 2,500 U.S. Participants.



Analysis

Type of Transaction:

Restricted Transaction
(Vendor Agreement)

Requirements:

- CISA security controls
- Data Compliance Program
- Audit
- 10-year records
- Contractual

5 Enforcement and Penalties:

- **Consequences of Non-Compliance**

Civil and Criminal Penalties

$ Civil Penalties

Maximum Civil Penalty

$368,136

per violation

OR

2× Transaction Value

whichever is greater

Pre-Penalty Process

DOJ issues a pre-penalty notice, allowing the alleged violator to respond before a final decision.

Criminal Penalties

Willful Violations

$1,000,000

maximum fine

OR

20 Years

imprisonment

Willful Standard

Requires knowing, intentional violation. Negligence is insufficient.

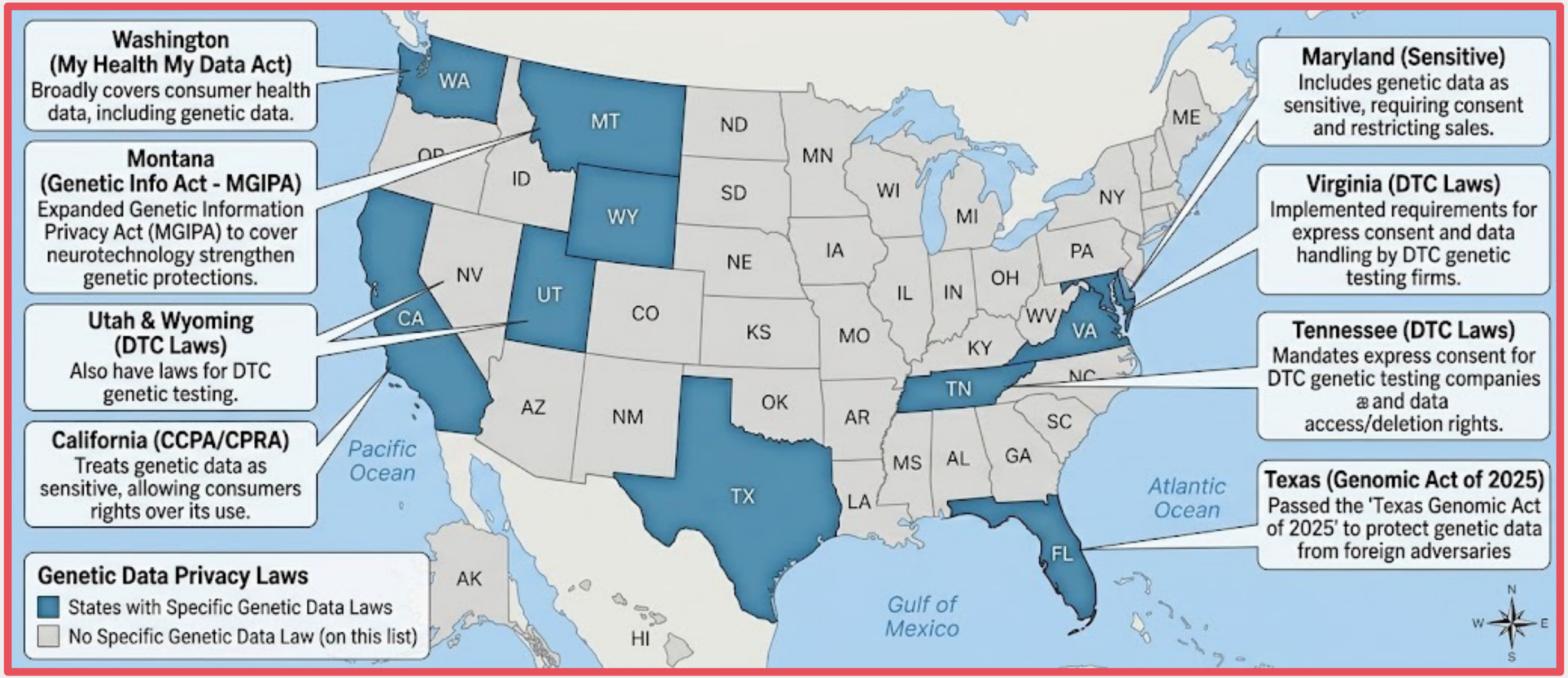
Conspiracy & Aiding

Conspiracy to violate the rule and aiding/abetting are also criminal.

6 Additional State Statutes:

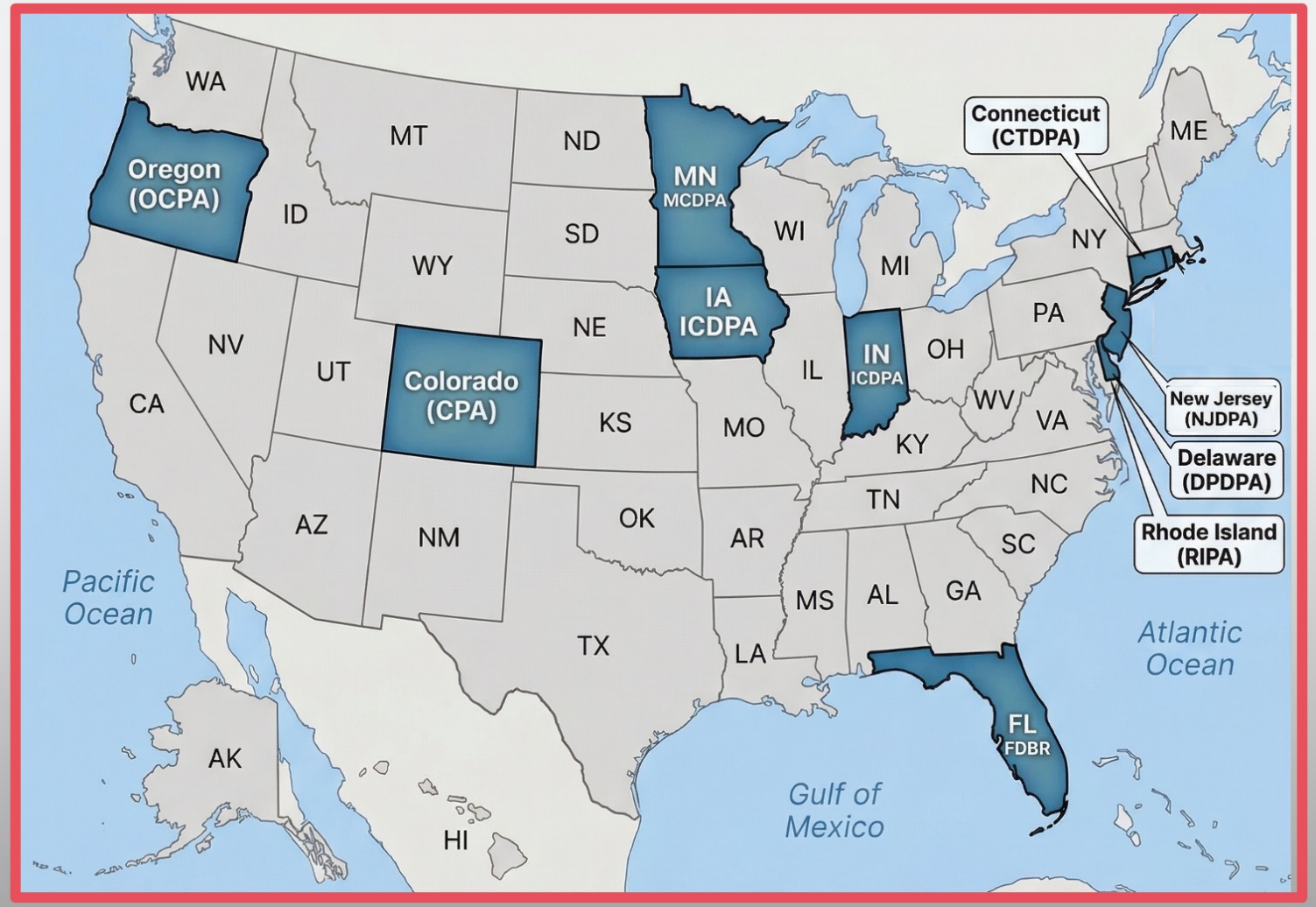
- Texas
- Montana
- Florida
- Etc.

Additional State Statutes:



States with Broader Privacy Laws Covering Genomics

Comprehensive data privacy laws in these states often classify genetic data as "sensitive" or similar, imposing stricter rules:



State Privacy Laws

- Active Data Privacy Law State
- No Comprehensive Law Specified

- Colorado (CPA)
- Connecticut (CTDPA)
- Delaware (DPDPA)
- Florida (FDBR)
- Indiana (ICDPA)
- Iowa (ICDPA)
- New Jersey (NJDPA)
- Oregon (OCPA)
- Rhode Island (RIPA)
- Minnesota (MCDPA)

Key Protections Offered

Express Consent: Opt-in requirements for collecting, using, or sharing genetic data.

Data Access & Deletion: Rights for consumers to view, correct, and delete their genetic data.

Restrictions on Sale: Prohibitions or limitations on selling genetic data.

Security Requirements: Mandates for data protection and breach notification.

Compliance Strategy:

- Strategic Steps for Institutions
- Dos and Don’ts for Compliance

Know Your Data

Data Inventory

- Gather all data that is received/collected, stored, and transferred.
- Evaluate whether the data falls within a defined category of bulk data.
- Label each data set and record with the appropriate category tag.

Threshold Calculation

- Determine quantity of records for each identified category.
- Compare the category calculations to the bulk data threshold.
- Flag all bulk data.

Data Flow Mapping

- **Who:** recipient identity.
- **What:** Data types and volumes transferred.
- **Where:** Geographic location of recipient.
- **Why:** Business purpose and legal basis.

Audit and Update Existing Relationships

Screening

- Screen all parties who have access to data including employees, vendors, and clients.
- Identify all parties who qualify as covered entities.
- Review and assess all agreements with identified entities.

Update Agreements

- Amend agreements that provide bulk data to foreign parties.
- Terminate rights for any entity where providing access would violate the Bulk Data Rule.
- Terminate access and permissions for any entity whose access would violate the Bulk Data Rule.

Security Controls

- Implement policies to screen new entities who gain access to bulk data.
- Implement appropriate security policies, especially for restricted transactions:
  - CISA security controls
  - Data Compliance Program
  - Audit
  - 10-year records

Conclusion

The Bulk Data Rule represents a fundamental shift in how the United States protects sensitive personal data from foreign adversaries. For hospitals and academic research institutions, compliance is not merely a legal requirement but a strategic imperative essential to protecting national security while continuing vital international collaboration.

The time to act is now. The 90-day enforcement grace period has ended. Full enforcement is underway. Institutions must move immediately to assess their data flows, screen their partners, implement security controls, and build comprehensive compliance frameworks—or face severe financial and criminal penalties.

This is not just about compliance. It is about protecting the nation's security while preserving the scientific and medical innovation that saves lives. The challenge is significant. The stakes are high. But with proper planning, robust governance, and sustained commitment, institutions can navigate this new regulatory landscape successfully.

Questions?

Connect with Our Presenter

ARE LLP

CHARLES R. MACEDO