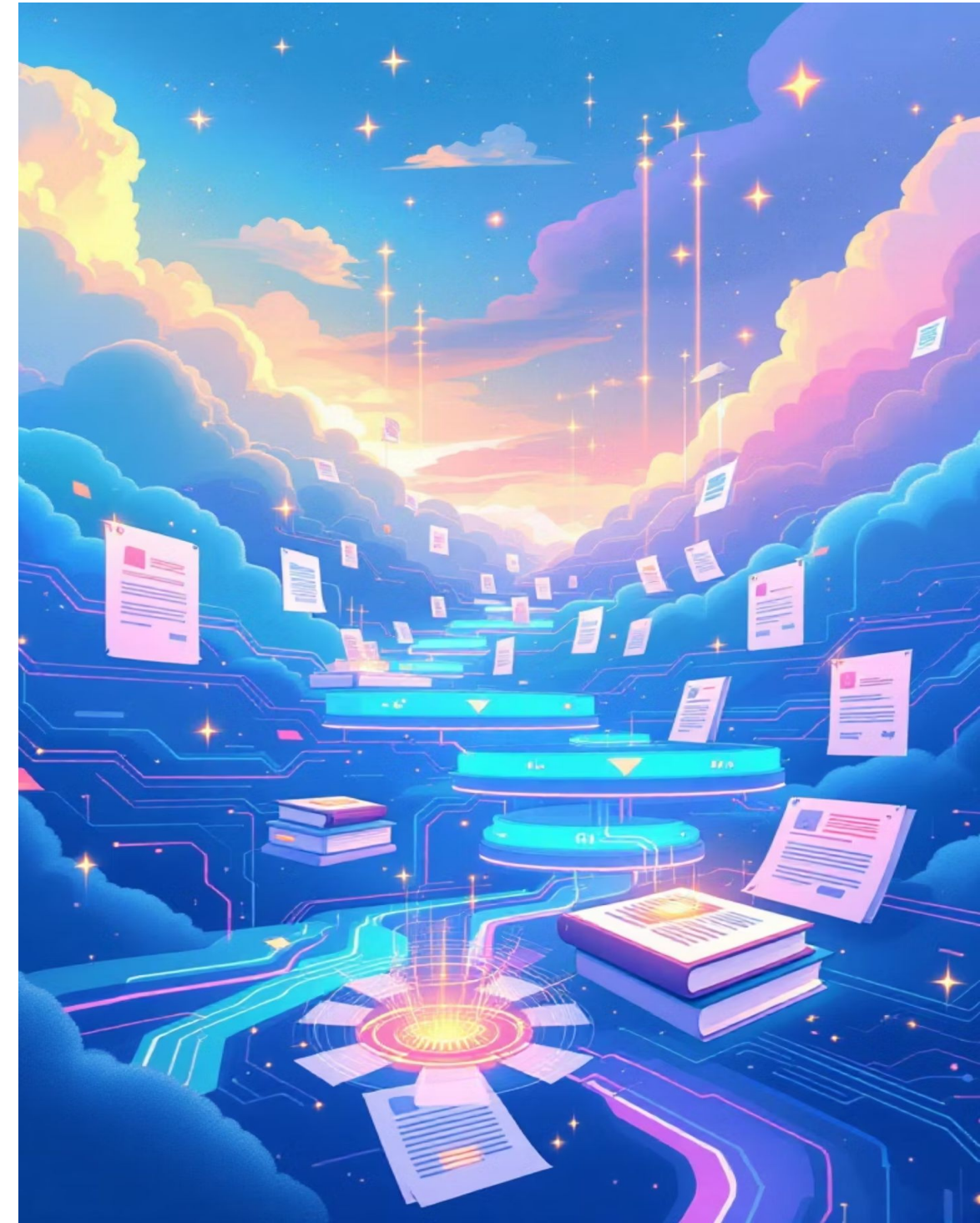


Legal Implications of a Permanent Digital Record

Navigating the intersection of technology, law, and accountability in the digital age



The Rise of Permanent Digital Records

Federal Mandate

Digital transformation requires permanent electronic recordkeeping
(NARA, 2023)

Regulatory

Framework

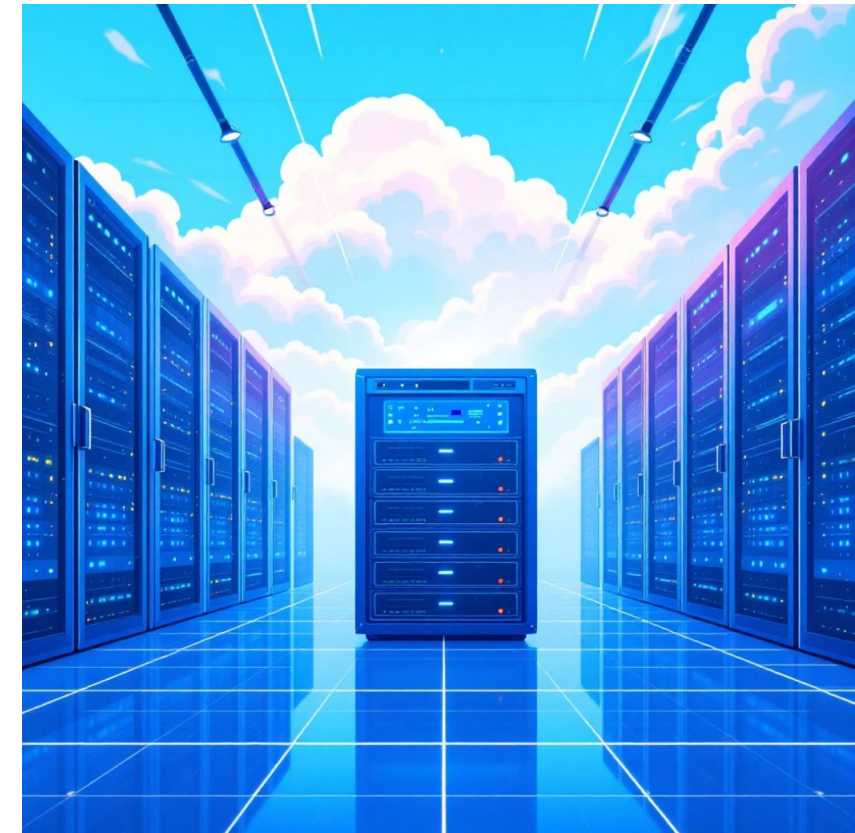
36 CFR § 1236 Subpart E governs digitising permanent paper records

Record Types

Text, maps, photos included; some media like film/audio excluded

Disposal Rules

Originals disposable only if digitisation meets strict standards



Legal Requirements for Digital Recordkeeping

Completeness & Accuracy

Records must meet federal standards for integrity and authenticity (NARA)

Source Retention

Original records may require retention despite digitisation due to legal or business needs

Mandatory Compliance

Federal Records Act and Sunshine Laws govern transparency and access

Non-Compliance Risks

Penalties, loss of transparency, and costly litigation threaten agencies



CHALLENGES

Challenges in Managing Digital Records Permanently

Expanding Scope

Beyond emails: texts, chats, social media require capture (Everlaw, 2024)

BYOD Risks

Security and privacy concerns with personal devices for work communications

Official Accounts

Need strict access controls and designated channels to ensure authenticity

Archiving Complexity

Capturing diverse communication channels comprehensively remains challenging

Authentication and Admissibility in Legal Proceedings

Authentication Required

Electronic records must prove authorship and integrity

Electronic Signatures

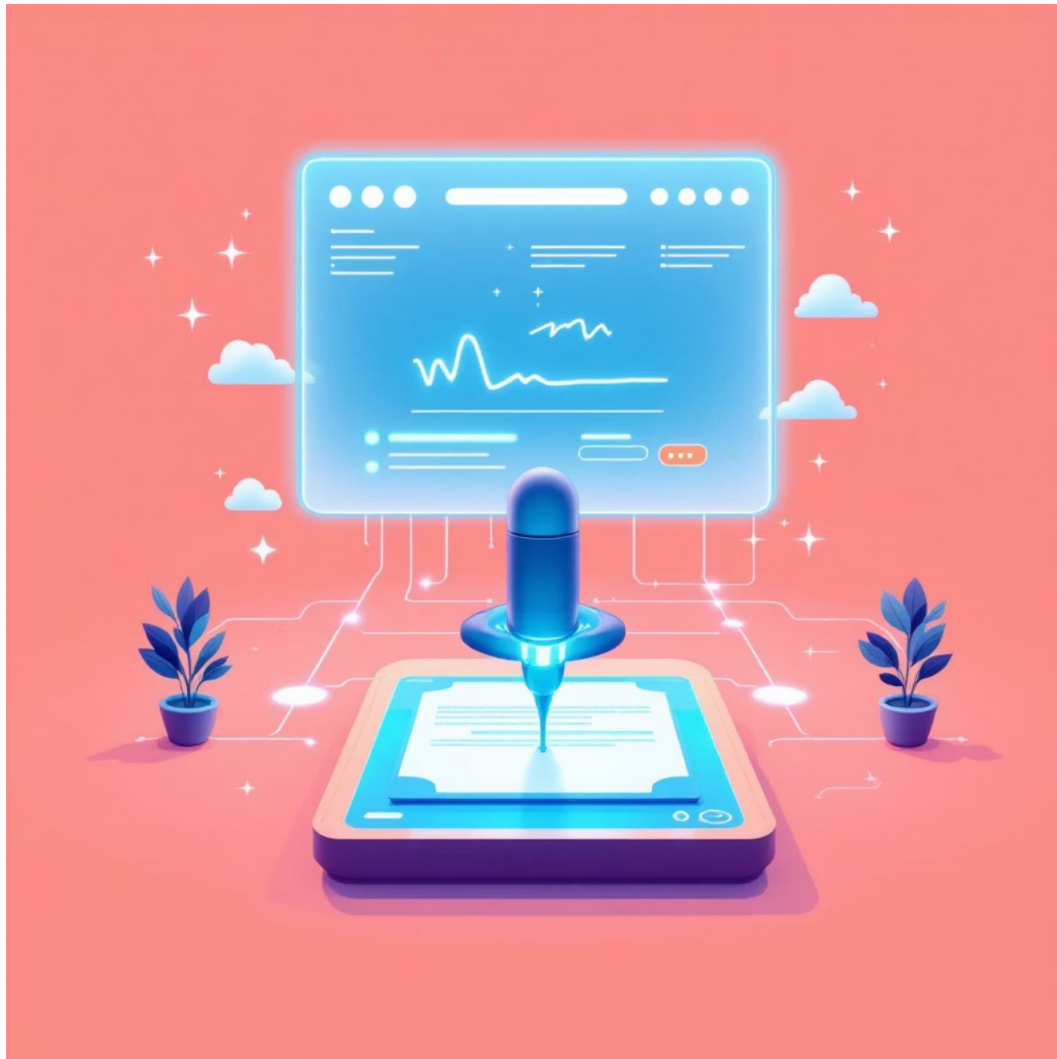
Accepted when verifying identity and complying with regulations

Custodian Certification

Health information managers and officials certify records for legal use

Court Admissibility

Proper certification ensures records serve as admissible evidence





 STANDARDS

Standards and Technologies for Trustworthy Digital Records



Trusted Systems

Follow ANSI, AIIM, and ISO standards (California Code)



Preferred Formats

PDF/A ensures long-term accessibility and integrity



Secure Storage

Compression and encryption protect against loss or alteration



Uniform Standards

Agencies adopt statewide or federal consistency protocols

Retention and Destruction Policies for Permanent Records



1

Indefinite Retention

Permanent records retained unless digitised per standards

2

Approved Digitisation

Original paper destroyed only after compliant digital conversion and backup

3

Duplicate Disposal

Copies destroyed when operationally unnecessary

4

Local Alignment

Policies must comply with administrative codes (e.g., San Francisco)

TRANSPARENCY

ACCOUNTABILITY

Transparency, Accountability, and Open Records Compliance

1

Public Trust Foundation

Digital records underpin government transparency and citizen confidence

2

Sunshine Law Requirements

Timely access to accurate digital records upon public request

3

Non-Compliance

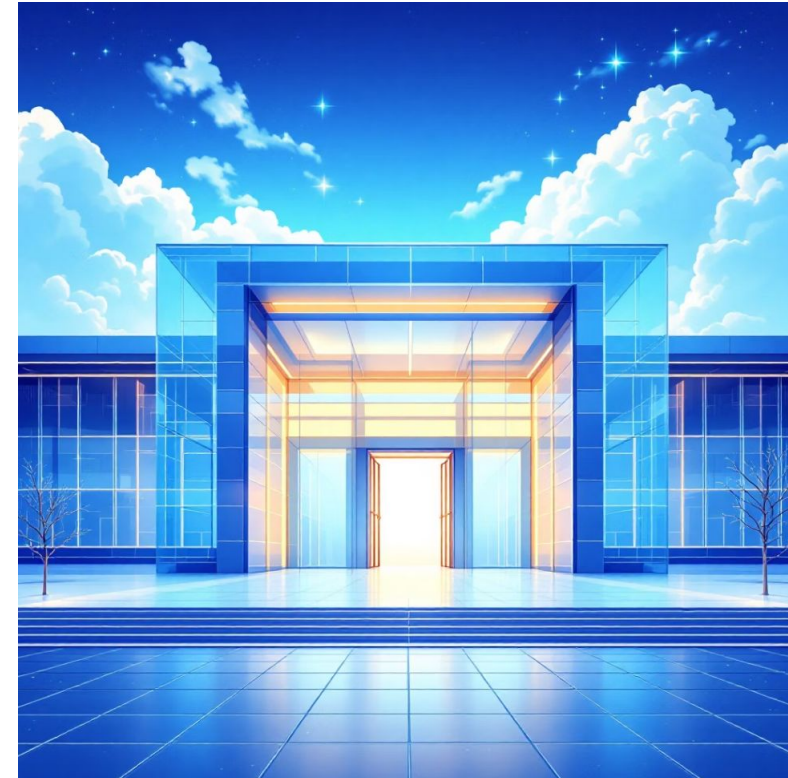
Consequences


Reputational damage and legal penalties threaten agencies

4


Cost Reduction

Effective archiving reduces expensive external eDiscovery processes



 BEST PRACTISES

Practical Steps for Agencies to Ensure Compliance

-  **Comprehensive Audits**
Review all communication channels and data sources systematically
-  **Clear Policies**
Implement guidelines on official account usage and BYOD management
-  **Staff Training**
Educate personnel on digital recordkeeping responsibilities and legal risks
-  **Technology Investment**
Deploy secure, comprehensive archiving and retrieval systems



Embracing the Permanent Digital Record Era

The future demands continuous adaptation to evolving digital communication landscapes

Essential Integrity

Permanent digital records vital for legal, operational, and historical purposes

Balanced Compliance

Success requires harmonising technology, policy, and legal frameworks

Proactive Management

Safeguards transparency, accountability, and evidence integrity

