BakerHostetler

Information Governance for Legal Practitioners – A Guide to Discussions with Clients

James A. Sherer

2023



This Photo by Unknown Author is licensed under CC BY-NC-ND

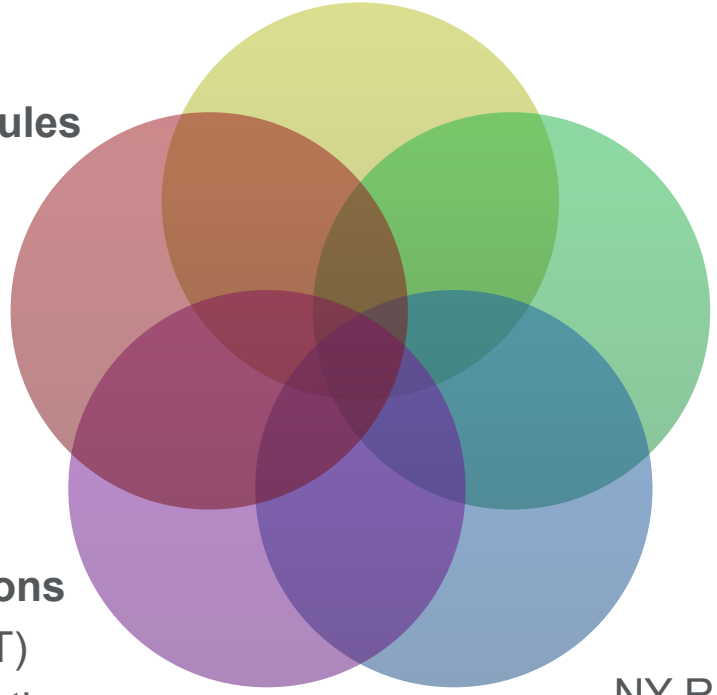
Agenda

- Information Governance and Records Overview
- An Operational Information Governance Program
- The Record Retention Policy and Schedule
- Roles and Responsibilities
- Handling Certain Information
- Legal Holds and Policy (and Practice) Exceptions
- Additional Resources

Why Information Governance?

US and International Privacy Laws
EU General Data Protection Regulation
California Consumer Privacy Act

Federal Laws and Rules
FTC
HIPAA
GLBA



NY Breach Notification Laws
N.Y. Gen. Bus. Law § 899-aa
N.Y. State Tech. Law § 208
(NY SHIELD Act)

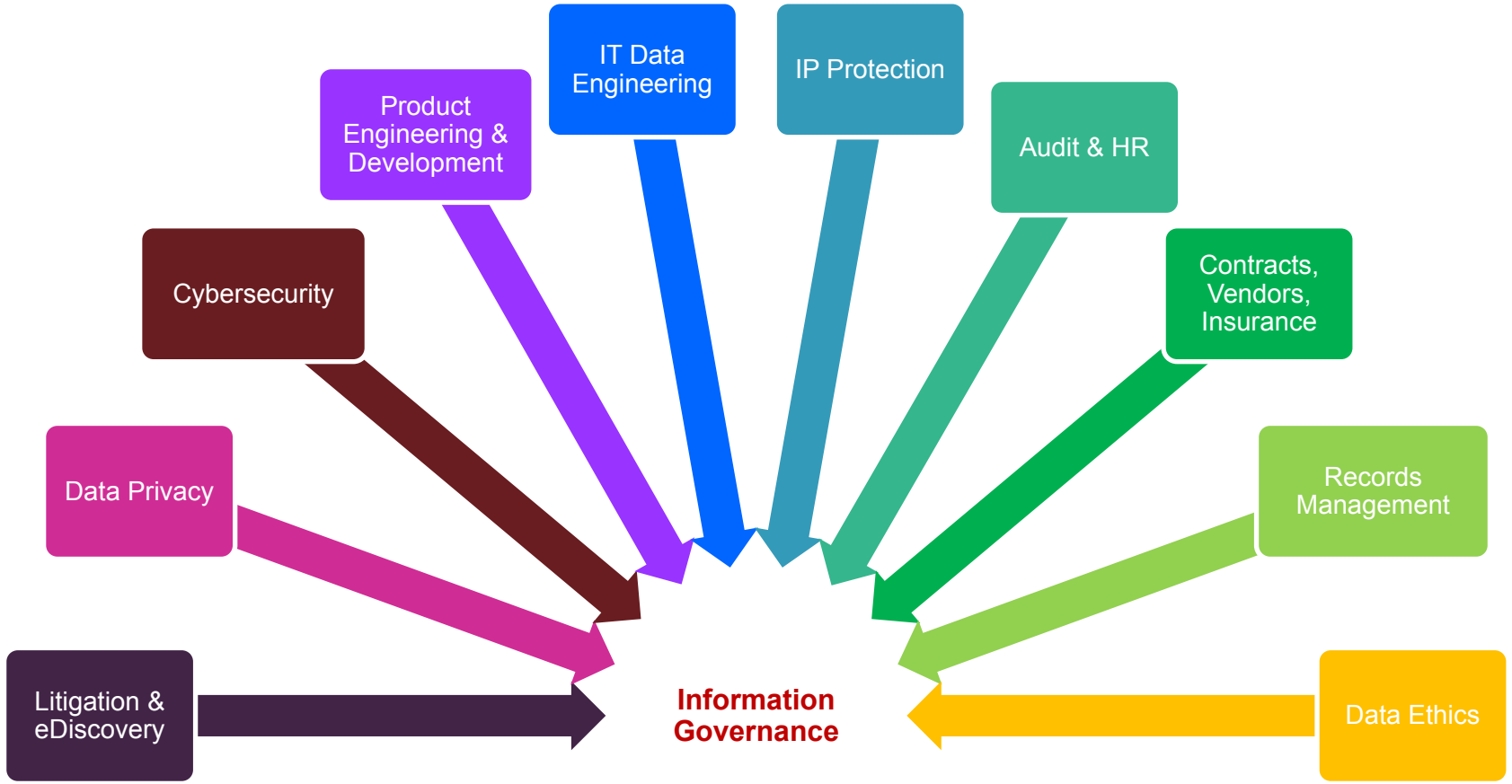
New York Laws & Regulations
NYC Local Law 144 (AEDT)
NYDFS Cybersecurity Regulation

Ethical Rules
ABA Model Rules
NY Rules of Professional Conduct

What is Information Governance?

The organization and management of corporate information through processes and controls

- Information is a valuable asset that must be handled appropriately
- Good information governance ensures we can access information when needed while reducing risks related to storage and security



Again, Why Information Governance?



Satisfy statutory and regulatory requirements



Harmonize approach across workstreams



Maximize value and utility of company data



Integrate new company systems and data



Reduce occurrence and costs of legal discovery and regulatory penalties



Enhance operational transparency

J. Sherer, T. Hoffman & E. Ortiz, *Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, e-Discovery, and Information Governance into Due Diligence Practices*, 21 RICH. J.L. & TECH. 5:15 (2015)
J. Sherer, T. Hoffman, E. Ortiz, K. Wallace & T. Satnick, *Merger and Acquisition Due Diligence II – The Devil in the Details*, 22 RICH. J.L. & TECH. 2:4 (2016)

What are Records?

Record:
Any information recorded in the course of a business activity that carries a legal, regulatory, or business retention requirement

- Records can exist in a variety of forms, including paper documents, electronic documents, video or digital images, graphic representations, and audio recordings.
- Not every piece of information or document is a record, but every record must be retained appropriately.
- Records management is a key component of information governance.

J. Sherer, J. Selby & J. Rovine, *Opting for a New Approach to Information Governance*, Bloomberg BNA–Digital Discovery & e-Evidence, Vol. 14, No. 482 (2014)

What is a Records Program Overview?

Scope

- Applies to all information collected and held at an organization, regardless of medium.

Roles & Responsibilities

- Everyone at an organization is responsible for properly handling information in accordance with the Records Retention Policy and other company policies.
- Records Coordinators will lead the efforts to ensure compliance.

Open Dialogue

- Asset Owners, Records Coordinators, and the IT Department must regularly communicate.

Compliance Verification

- All organizational team members must understand the information governance program.

What is a Records Retention Schedule?

Describes how an organization retains and disposes of information processed in the course of business activities.

Records retention is determined by legal requirements, industry standards, contractual requirements, and best practices.

Constitutes best practices as well as exceptions to normal operation.

12 CFR § 1006.100(a), promulgated under the Fair Debt Collection Practices Act (FDCPA), prescribes Active + 3-Year retention for “records that are evidence of compliance or noncompliance with the FDCPA”

Records Retention Schedule (Continued)

- Lists the types of records the organization maintains and the length of time the records must be kept before they are eligible for destruction.
- Retention periods are based on legal and regulatory requirements, as well as business needs.
- Prescribed retention periods may be adjusted but should consider a directed approach to do so.
  - Note many organizations employ a “federated” approach

How do Roles and Responsibilities Work?

- Every employee may be responsible for effectively harnessing the information collected.
- Information must be accurately stored and safely handled.

- Each business unit may utilize a Records Coordinator to facilitate compliance with Records/Data Retention Policy.
- Records Coordinators will regularly communicate with IAOs to ensure appropriate measures are being followed.
- Records Coordinators should work with the IT Department to align records management needs with IT infrastructure.

How do Repositories Work?



Records Coordinators will designate appropriate repositories.



Everyone may be responsible for saving electronic records in the appropriate locations.



Records may not be saved on computer desktops or personal computers.

Handling Transient Information

- An organization may deploy an email use policy.
- Email is primarily intended to be used as a communication tool and should not be treated as a formal repository for records.
- Any records contained in email that are not merely duplicates should be placed in their appropriate repositories.

Example:
A signed contract is emailed to you.
The contract should be saved in the appropriate repository so your team members can access the contract, as needed, and the contract can easily be found in the future.

J. Sherer, A. Singer & S.B. Barnes, *Picking up the Slack™: Legal and Information Governance Considerations for New(er) Technologies*, Kathmandu eDiscovery Lecture Series (2018), 25 RICH. J.L. & TECH. 4 (2019)

Legal Holds – the Exceptional Exceptions

Legal Hold: Suspending the disposal of information to preserve such information for a legal purpose

- The Legal Department may circulate notices identifying information that needs to be retained for a legal purpose, **even if that information would otherwise be eligible for destruction**.
- These Notices may be circulated to preserve information for litigation, audits, regulatory investigations, or other situations where the Legal Department requires ongoing access to certain information.
- Recipients of a Legal Hold notice must acknowledge and comply with the request.
- Employees who fail to preserve information subject to a hold may be subject to disciplinary action, up to and including termination.

FRCP Rule 37(e); *see also Armory v. Delamirie* (1722); 2023 WL 2673109, No. 21-md-02981-JD (N.D. Cal. Mar. 28, 2023)

Other Resource Considerations

- Contact your Records Coordinator with questions related to your business unit
- The complete listing of all Records Coordinators can be found here: [Intranet Link]
- Questions about the Records Retention Policy or compliance with the Policy may be directed to the Legal

(Past) Future Considerations

- Auto-classification uses meta-data and rules (algorithms) to recognize document types, engage in content analytics, and appropriately tag and index data, among other things (e.g., an email filter that recognizes and sorts spam from valued email).
- Auto-classification in RIM arose in the early to mid-2000s, as information management professionals acknowledged that record owners were neither quick nor accurate in deciding what information qualified as a record or in assigning disposal dates under an appropriate classification system.
- In eDiscovery, auto-classification is sometimes called predictive coding or technology-assisted review. Regardless of the name, auto-classification application in eDiscovery teaches computers to assign tags to information, just as in information governance.

epiq, *Autoclassification Aids Information Governance* (August 7, 2018)

(Past) Future Considerations

- Sensitive Information Types -
  - Use E3 license to identify sensitive information
  - Create your custom Sensitive Information Types and then apply Data Loss Prevention policies
  - Automate retention or protection for sensitive information through an E5 add-on license
- Trainable Classifiers – identify unstructured content (e.g., contracts, resumes, decision memos, etc.) through E5 add-on license
- SharePoint Syntex -
  - Identify semi-structured information and automate the extraction of data from files with license-add on with E3 or E5
  - Automate identification and classification of semi-structured information (similar to Trainable Classifiers), but also automate data extraction.
  - Auto-classification approach: machine teaching with minimum 5 positive and 1 negative samples for auto-classification, but more for data extraction

A. Skjekkeland, *Automate Information Governance with M365 AI and Machine Learning* (May 24, 2021)

Present Considerations – from Records to Data

- Manage Data at Scale
  - The average company manages hundreds of terabytes of data - For data to perform as an asset rather than a liability, it must be located, classified, cleansed, and monitored.
  - With so much data entering the organization so quickly from so many disparate sources, conducting those data tasks manually is not feasible.
- Build Visibility to Ensure Trustworthy Data
  - Organizations making accurate data-driven decisions need clean, reliable data.
  - AI-powered analysis is only useful if based on complete and accurate data sets.
  - This requires visibility into relevant data, and back-end exhaustive checks for errors, duplicates, and outdated information.
- Secure Data Assets and Achieve Compliance
  - Privacy regulations, for example, require that organizations take all reasonable measures to keep confidential data safe from unauthorized access.

James A. Sherer



Partner
jsherer@bakerlaw.com

James Sherer is co-chair of the Emerging Technology Team and leads BakerHostetlers' Information Governance and AI practice efforts. His work focuses on litigation; discovery management processes; enterprise risk management; records and information governance; data privacy, security and bank secrecy; artificial intelligence and algorithmic transparency; technology integration issues; and related merger and acquisition diligence.

Prior to joining BakerHostetler, James worked as in-house litigator with a Fortune 500 company and previously practiced litigation in New York. He maintains the CIPP/US, CIPP/E, CIPM, FIP, and PLS data privacy professional credentials, the CIP and IGP information governance designations, the UCLA Extension Global Cyber Institute's Cybersecurity Certification, and the CEDS and eDPC eDiscovery specialist credentials. James is also a member of The Sedona Conference® Working Groups One, Six, and Eleven; and writes and presents on e-discovery, information governance, privacy, investigation, and merger and acquisition issues.

James holds an A.B. from the University of Michigan, an M.B.A. in Finance from Central Michigan University, and a J.D. from the Columbia University School of Law.