Richmond Journal of Law and Technology

Volume 20 | Issue 2 Article 2

2014

The Compliance Case for Information Governance

Peter Sloan

THE COMPLIANCE CASE FOR INFORMATION GOVERNANCE

By Peter Sloan[*]

Cite as: Peter Sloan, *The Compliance Case for Information Governance*, 20 RICH. J.L. & TECH. 4 (2014), http://jolt.richmond.edu/v20i2/article4.pdf.

I. INTRODUCTION

[1] In an increasingly convoluted information environment, organizations strive to manage information-related risks and exposures, minimize information-related costs, and maximize information value. The inadequacy of traditional strategies for addressing information compliance, risk, and value is becoming clear, and so too is the need for a better, more holistic approach to governing the organization's information.[1]

[*] Peter Sloan is a partner at the law firm Husch Blackwell LLP and a founding member of the firm's Information Governance Group. For over a decade he has focused his practice on how companies can best manage their records and information. He is an ARMA International member and has been a long-standing participant in Working Group I of The Sedona Conference, contributing to several of its publications, including *The Sedona Conference Commentary of Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible* (2009) and most recently, *The Sedona Conference Commentary on Information Governance* (2013). He has helped companies across a wide variety of industries create, validate, and update records retention schedules; implement information compliance systems; develop legal hold processes; and deploy risk management and information governance approaches to information. The author thanks the JOLT staff and also his colleague and paralegal extraordinaire Kerri Steffens, who has applied information governance controls to the citations in this article. Any errors remain the responsibility of the author.

[1] When discrete departments or groups within an organization make autonomous decisions about information, inconsistencies and problems can result. Similarly, information-related decisions and actions driven by insular information disciplines (such as records and information management, privacy and data security, or litigation

[2] Information governance is "an organization's coordinated, inter-disciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value."[2] This definition highlights three key aspects of an organization's relationship with information. First, the organization is subject to information legal requirements, such as statutory, regulatory, and contract requirements, which must be satisfied. Second, the organization faces information-related risks[3] (the likelihood that an event or circumstance will occur that could cause harm to the organization) that need to be controlled so that the resulting harm is avoided, minimized, or otherwise managed. Last, the organization's information and related practices have an economic impact, or value, that the organization can address by controlling information-related costs, optimizing information-related efficiencies, and maximizing the inherent value of its information.[4]

[3] Of these three elements—compliance, risk, and value—the latter two most commonly take center stage when organizations contemplate the information governance approach. Obtaining management approval, commitment, and budget for information governance usually involves

preservation) can create inefficiencies and risks for the organization as a whole. *See* THE SEDONA CONFERENCE, THE SEDONA CONFERENCE COMMENTARY ON INFORMATION GOVERNANCE 5 (Conor R. Crowley ed., 2013).

[2] *Id.* at 2.

[3] In the formal discipline of risk management, the definition of "risk" has evolved to mean the "effect of uncertainty on objectives." INT'L ORG. FOR STANDARDIZATION, ISO 31000, RISK MANAGEMENT—PRINCIPLES AND GUIDELINES § 2.1 (2009). While risk remains the combination of (1) the consequences of an event or change of circumstances and (2) the likelihood of such an occurrence, "effect" is defined as either a negative or positive deviation from the expected. *Id.* at § 2.1 nn. 1, 4. This Article uses the more traditional connotation of risk, which is the likelihood of a negative or harmful result.

[4] *See* THE SEDONA CONFERENCE, *supra* note 1, at 6.

making a "business case,"[5] built upon what colloquially can be referred to as carrots and sticks. Carrots include potential cost savings, efficiencies, and opportunities to reap additional value from the organization's information and information processes.[6] Sticks are examples of dire information-related exposures, coupled with resulting costs and harm should they occur. These carrots and sticks correspond to information value and information risk.[7] Business case considerations of risk and value indeed can be persuasive arguments for what the organization *should* do. But missing from this business case equation is the first element, legal compliance, which converts *should* do into *must* do.[8]

[4] The above definition of information governance also captures its coordinated, interdisciplinary nature. The salient feature of the information governance approach is that it compels organizations to take a broad, inclusive view of information issues, and to act accordingly. Information governance bridges across entrenched silos in the organization's various departments and functions, including Legal, IT, Compliance, Records Management, and lines of business or operations, thereby avoiding parochial decisions regarding information.[9] The information governance approach also causes organizations to reconcile various information-focused disciplines, such as records and information

[5] *See generally* Charles R. Ragan, *Information Governance: It's a Duty and It's Smart Business*, 19 RICH. J.L. & TECH. 12 (2013), http://jolt.richmond.edu/v19i4/article12.pdf (discussing the business case for information governance).

[6] *See* THE SEDONA CONFERENCE, *supra* note 1, at 6.

[7] *See id.* at 2, 4.

[8] Doug Cornelius, *McNulty Keynote on a Tale of Two Sectors*, COMPLIANCE BUILDING (June 4, 2009, 2:16 PM), http://www.compliancebuilding.com/2009/06/04/mcnulty-keynote-on-a-tale-of-two-sectors/ ("The cost of non-compliance is great. If you think compliance is expensive, try non-compliance.").

[9] *See* THE SEDONA CONFERENCE, *supra* note 1, at 4.

management, privacy and data security, intellectual property, and litigation preservation.[10]

[5] Though organizations often pursue these information-focused disciplines on an autonomous basis, the legal requirements in the disciplines of records and information management, privacy and data security, intellectual property, and litigation preservation seldom operate in a vacuum. Instead, such legal requirements interrelate and interact across their respective disciplines' boundaries. Thus, when information is kept longer than required by records retention laws, the likelihood increases for a security breach under data security laws or for a disclosure jeopardizing trade secret status; also, the volume of information subject to subsequent legal holds increases.[11] Disposal of information in compliance with records retention and data security laws may violate litigation preservation requirements.[12] And the processing and handling of information preserved and produced in litigation inevitably has an impact upon retention and records management compliance, and additionally may

[10] *Id.* at 1.

[11] *See id.* at 32.

[12] *See* Kenneth J. Withers, *Risk Aversion, Risk Management, and the "Over-Preservation" Problem in Electronic Discovery*, 64 S.C. L. REV. 537, 578 (2013) (discussing the necessity of considering the risk of data loss and consequent violation of "the duty of preservation" before formulating an information governance program); *see also* Bennett B. Borden et al., *Four Years Later: How the 2006 Amendments to the Federal Rules Have Reshaped the E-Discovery Landscape and Are Revitalizing the Civil Justice System*, 17 RICH. J.L. & TECH. 10, ¶ 48 (2011), http://jolt.richmond.edu/v17i3/article10.pdf (explaining preservation obligations and recognizing that "[e]ven with an effective information governance plan and protocols in place to recognize a triggering event, the preservation burden can be substantial"); The Sedona Conference, *The Sedona Conference Commentary on Legal Holds: The Trigger & the Process*, 11 SEDONA CONF. J. 265, 274 (2010) (explaining the primacy of legal holds and suggesting that organizations have electronically stored information management policies that "include provisions for implementing procedures to preserve documents and electronically stored information related to ongoing or reasonably anticipated litigation").

have intellectual property and privacy and data security repercussions. This interplay of information legal requirements fosters the interdisciplinary approach of information governance. And while information-related compliance requirements create synergies for information governance, certain information legal requirements explicitly mandate that organizations establish foundational elements of an information governance program.[13]

[6] This Article first provides a summary overview of information-related legal requirements. Next, this Article identifies specific legal requirements that expressly compel organizations to establish crucial building blocks for an effective information governance program. Last is a discussion of how information compliance requirements provide compelling synergies for the information governance approach.

II. OVERVIEW OF INFORMATION LEGAL REQUIREMENTS

[7] Major categories of information legal requirements include laws regarding records retention and electronic recordkeeping, privacy and data security, intellectual property, and litigation preservation.

A. Records Retention

[8] Tens of thousands of record retention legal requirements reside in the statutes and regulations of the federal government, the fifty states, the District of Columbia, and the U.S. territories.[14] Legal requirements include regulations mandating that specific records be kept for an explicit

[13] *See infra* Part III.

[14] This observation is based upon the author's many years of caffeine-fortified experience creating and validating records retention schedules for organizations across a wide range of industries.

time period,[15] for a time period after a triggering event,[16] or simply that the record be maintained, without providing an explicit retention period.[17]

[9] Records retention legal requirements cover the gamut of an organization's operations and functions, including such areas as accounting, compliance, environmental, facilities, finance, general administration, government relations, health and safety, information technology, legal, entity governance, operations, personnel, public relations and marketing, procurement, transportation, and tax.[18]

[10] For example, consider records retention for contracts. Organizations in certain regulated industries have explicit legal requirements for retaining contract records. Thus, securities brokers and dealers must retain all written agreements relating to their business for three years;[19] registered investment advisers must retain all written

[15] *See* 29 C.F.R. § 1627.3(a) (2013) (requiring employers to retain payroll records for three years).

[16] *See* 29 C.F.R. § 1627.3(b)(1) (requiring employers to retain specified employment records until one year after the date of the related personnel action).

[17] *See* 26 C.F.R. § 1.6001-1(e) (2013) (requiring taxpayers to retain supporting tax records "so long as the contents thereof may become material in the administration of any internal revenue law").

[18] Such requirements are generally embedded in the wide range of federal and state statutes and regulations that govern the various functional activities of organizations. For example, tax codes and regulations provide retention requirements for an organization's books and records of accounting and transactions, *see, e.g.*, 26 U.S.C. § 6001, and health and safety codes and regulations, to the extent applicable, provide retention requirements for employee medical and exposure records, *see, e.g.*, 29 C.F.R. 1910.1020. In highly-regulated industries, the rules of the primary federal or state regulator may also cover recordkeeping for a broad range of the organization's functions. *See, e.g.*, 17 C.F.R. §§ 240.17a-3 - 240.17a-4 (pertaining to brokers and dealers); 18 C.F.R. § 125.3 (regulating power utilities); 49 C.F.R. pt. 379 app. A. (regulating motor carriers).

[19] *See* 17 C.F.R. § 240.17a-4(b)(7) (2013).

agreements related to their business for five years after fiscal year-end;[20] power utilities, natural gas companies, and their holding companies must retain service contracts and contracts for purchase or sale of product for four years after contract expiration;[21] motor carriers must retain service contracts for three years after expiration;[22] Medicare Part D plan sponsors must retain contract records for ten years;[23] and so forth across the wide range of regulated industries.[24] In addition, specifically regulated activities of general organizations can also trigger retention requirements. For example, if a business has a self-administered health benefits plan, the health plan may have covered entity status under the Health Insurance Portability and Accountability Act (HIPAA), thereby making applicable the HIPAA requirement that business associate contracts be retained for six years after last in effect.[25] Also, state laws frequently provide overlapping contract records retention requirements that may exceed prescribed federal retention periods.[26]

[20] *See* 17 C.F.R. § 275.204-2(a)(10), (e)(1).

[21] *See* 18 C.F.R. §§ 125.3.3(a)-(b), 225.3.3(a)-(b), 368.3.3(a) (2013).

[22] *See* 49 C.F.R. pt. 379 app. A. tbl.A § 5(a)-(b) (2012).

[23] *See* 42 C.F.R. § 423.505(d)(2)(iv)-(vi) (2012).

[24] The granular applicability of such industry-specific retention requirements is remarkable. *See, e.g.*, IOWA ADMIN. CODE r. 21-91.11(7)-(9) (2013) (requiring Iowa grain dealers to retain credit-sale contracts and acknowledgments, including cancelled credit-sale contracts, for six years).

[25] 45 C.F.R. §§ 164.308(b)(3), 164.316(b)(2)(i), 164.502(e)(2), 164.530(j)(2) (2012).

[26] For example, while power and gas utilities regulated by the Federal Energy Regulatory Commission have a four year records retention requirement for expired service contracts and product contracts, several states, such as California, Illinois, and Massachusetts, require power and gas utilities to retain such contracts for six years after expiration. *See* CPUC Resolution FA-570 (1976) (adopting Fed. Power Comm'n Order No. 450, which incorporated the 1972 edition of 18 CFR §§ 125, 225 (although the CFR has been updated since, California continues to apply the requirements of the 1972 federal

[11] If the organization's industry and operations are such that no explicit legal requirement applies for contract records retention, the organization's contracts nevertheless are documentation of legal rights and obligations, and they should be retained after expiration for a legally prudent period of time to allow for the possibility of residual contract disputes. Statutes of limitations for contract claims are therefore a legal consideration for contract retention, and organizations may determine a legally prudent period of time to retain expired contracts, based upon applicable contract statutes of limitations and the practical likelihood of contract disputes after contract expiration.

B. Electronic Recordkeeping

[12] Federal and state laws allow most required records to be retained in electronic form. For example, contracts, agreements, and other transaction records, despite statutes of frauds and other laws to the contrary, may generally be retained electronically, pursuant to the Federal Electronic Signatures in Global and National Commerce Act (E-Sign Act),[27] and under state laws that either contain equivalent provisions or that adopt the Uniform Electronic Transactions Act (UETA).[28]

regulation)), ILL. ADMIN. CODE tit. 83, § 420 app. A.9(a)-(b), § 510 app. A.9(a)-(b); 220 MASS. CODE REGS. 75.05(7)(a)-(b) (2013).

[27] Transactions in or affecting interstate or foreign commerce are generally valid and enforceable under the E-Sign Act with signatures, contracts, and other related records in electronic form, despite laws to the contrary. *See* 15 U.S.C. § 7001(a) (2012). Laws that require retention of contracts, cancelled checks, or other records of such transactions are satisfied by retaining an electronic record that accurately reflects the information set forth in the contract, check, or other transaction record, and that remains accessible to all persons legally entitled to access, for the required period, in a form capable of accurate reproduction. *See* § 7001(d).

[28] Forty-seven states, the District of Columbia, Puerto Rico, and the Virgin Islands have adopted the U.E.T.A. Illinois, New York and Washington have not adopted the U.E.T.A., but instead have their own statutes pertaining to electronic transactions, records, and signatures. Under the U.E.T.A., the enforceability of contracts, signatures,

Exceptions to the reach of the E-Sign Act and the UETA include laws governing the creation and execution of wills, codicils, or testamentary trusts; state laws governing adoption, divorce, or other matters of family law; Uniform Commercial Code requirements other than Sections 1-107 (waiver of claims after breach), Section 1-206 (statute of frauds for sale of certain personal property), Article 2 (sales), and Article 2A (leases); court orders, notices, or official documents required to be executed in connection with court proceedings; certain required notices, such as for cancellation of utility services, repossession or foreclosure under credit agreements secured by an individual's primary residence, cancellation of health or life insurance benefits, and certain product recalls; and documents required for transportation or handling of hazardous or toxic materials.[29]

[13] Though electronic recordkeeping is generally permissible under federal and state laws, a wide variety of legal requirements apply to the manner in which required electronic data is stored, indexed, and maintained, including how required records are converted from original paper form to official recordkeeping in digital media. Thus, Internal

---

and records of covered transactions cannot be denied solely because they are in electronic form, and electronic signatures and electronic records related to such transactions will satisfy laws requiring signatures and writings. U.E.T.A. § 7 (1999). The U.E.T.A. provides that

> [i]f a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which: (1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and (2) remains accessible for later reference.

§ 12(a). The U.E.T.A. also allows record holders to convert original records of covered transactions to an electronic form meeting the above conditions and thereafter to destroy the original (paper) record. *See* § 12(d), cmts. 3, 5.

[29] *See* 15 U.S.C. § 7003(a)-(b); U.E.T.A. § 3 (1999).

Revenue Service records retention requirements may be satisfied by electronic recordkeeping in compliance with IRS Revenue Procedure 97-22 (electronic storage systems) and IRS Revenue Procedure 98-25 (automatic data processing systems) if various electronic recordkeeping requirements are met.[30] If required conditions are satisfied, completed I-9 forms and supporting employment eligibility documentation

[30] Under IRS Revenue Procedure 97-22, taxpayers may maintain required records in an electronic storage system that either images their hard copy records, or the transfer of original electronic data to an electronic storage media, such as optical disc. DEP'T OF THE TREASURY, INTERNAL REVENUE SERV., REV. PROC. 97-22 §§ 1, 3.01(1997). The electronic storage system must ensure an accurate and complete transfer of the original records to the electronic storage media and "must also index, store, preserve, retrieve and reproduce the electronically stored [records]." § 4.01(1). Revenue Procedure 97-22 imposes various requirements for such systems, including "reasonable controls to ensure integrity, accuracy, [] reliability," and prevention and detection of unauthorized activities or events; a compliant inspection and quality assurance program; a compliant indexing and retrieval system; the ability to reproduce legible and readable hard copy reproductions and video display; and an audit trail between the general ledger and the source documents. § 4.01(2)-(4). Taxpayers also must retain complete descriptions of the electronic storage system, system procedures for use, and the indexing system. § 4.01(5). Under IRS Revenue Procedure 98-25, covered taxpayers must retain machine-sensible records (data in electronic format intended for use by a computer, such an automated data processing system) they create in the ordinary course of business or to establish return entries. DEP'T OF THE TREASURY, INTERNAL REVENUE SERV., REV. PROC. 98-25 §§4.06, 5.01 (1998). "The taxpayer's machine-sensible records must provide sufficient information to support and verify" the taxpayer's return entries and determine the correct tax liability, by reconciling with the taxpayer's books and return through an audit trail, and must include sufficient transaction detail. § 5.01(2)-(3). Such taxpayers must maintain and make available to the Internal Revenue Service documentation of the business processes that create, modify, and maintain the machine-sensible records, that provide an audit trail to support and verify return entries and determine the correct tax liability, and that evidence the records' authenticity and integrity. § 6.01. Taxpayers must also retain documentation of formatting, field, and file descriptions for each retained file, evidence of periodic checks for data loss, evidence of reconciliation with the taxpayer's books and returns, and change management documentation. § 6.03-6.04. State tax regulations contain similar requirements for electronic storage of supporting tax records. *See, e.g.*, N.Y. COMP. CODES R. & REGS. tit. 20, § 2402.2 (2013).

may be retained in electronic media by original electronic creation or by conversion of original paper documents to electronic format.[31] Regulations under the Employee Retirement Income Security Act (ERISA) allow retention of pension and welfare benefits records in electronic media if the electronic recordkeeping system has adequate controls and if adequate records management practices are established and implemented, such as labeling procedures, secure storage environments, backup processes, and a quality assurance program.[32]

[14] Various regulated industries are subject to their own, specific requirements for electronic recordkeeping systems. Thus, securities brokers and dealers, investment companies, and investment advisers that use electronic storage media for required records must comply with mandated systems requirements and must have an audit system for accountability regarding records input and changes.[33] Power and gas utilities and their holding companies must have documented internal control procedures to assure reliability of and ready access to required data

[31] The federal I-9 regulations require that I-9 forms and supporting documentation created in or converted to electronic media must have an electronic generation or storage system that includes "[r]easonable controls to ensure the integrity, accuracy[,] reliability" of required records and prevention and detection of unauthorized activities or events; a compliant inspection and quality assurance program; a compliant indexing and retrieval system; and the ability to reproduce legible and readable hard copies and video display. 8 C.F.R. § 274a.2(e)(1)-(2) (2012). Such employers must retain documentation of the business processes that create, modify, and maintain the retained I-9 forms, and that establish authenticity and integrity, such as audit trails. § 274a.2(f). There must also be an effective security program that ensures only authorized persons have access to electronic records; provides backup and recovery; provides employee security training; and creates secure and permanent documentation (date, identity, and action taken) whenever the electronic record is created, completed, updated, modified, altered, or corrected. § 274a.2(g).

[32] 29 C.F.R. §§ 2520.107-1(b), 4000.53 (2013).

[33] 17 C.F.R. §§ 240.17a-4(f), 270.31a-2(f), 275.204-2(g) (2013).

stored on machine-readable media, and they must document and verify for accuracy media transfers of required data.[34] Federal contractors maintaining required information as computer data must have procedures in place to "maintain the integrity, reliability, and security" of the computer data; must establish procedures to ensure that any imaging process for required records preserves accurate images and that the imaging process is reliable, secure, and maintains the record's integrity; and also must maintain an effective indexing system.[35]

C. Privacy and Data Security

[15] United States federal and state privacy and data security laws include requirements for data security safeguards, breach notification, and privacy notifications and consents.

[16] First, organizations must provide data security for the information protected under the particular legal scheme, with adequate administrative, physical, technical, and organizational safeguards. Thus, HIPAA covered entities and their business associates must ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) they create, receive, maintain, or transmit, in compliance with the HIPAA Security Standards.[36] Financial institutions under the Gramm-Leach-Bliley Act must protect nonpublic personal information about their customers by developing and implementing a written, comprehensive information security program containing appropriate administrative,

[34] 18 C.F.R. §§ 125.2(d), 225.2(d), 368.2(e) (2013).

[35] 48 C.F.R. §§ 4.703(c)-(d) (2012). The Federal Acquisition Regulations also, and anomalously, require that original paper records compliantly converted to official electronic recordkeeping through scanning to electronic media must nevertheless be retained for one year after such scanning is performed. § 4.703(c)(3).

[36] *See* 45 C.F.R. pt. 164, subpt. C (2012).

technical, and physical safeguards.[37] Confidentiality requirements are also embedded in federal laws applicable to employers generally, such as regulations under the Family Medical Leave Act,[38] the Americans With Disabilities Act,[39] and the Genetic Information Nondiscrimination Act,[40] as well as Occupations Safety and Health Administration regulations.[41]

[17] Several states require organizations with protected personal information ("PII") of state residents to implement and maintain reasonable security procedures and practices to protect such PII from unauthorized access, destruction, use, modification, or disclosure. The Massachusetts regulatory scheme is the most detailed—compelling such entities to implement both a comprehensive information security program with "administrative, technical, and physical safeguards," and also an information security program with specified data security protections.[42] A majority of states have laws requiring organizations with PII to take reasonable measures to protect such information when it is disposed of or discarded.[43] While some such states require organizations to have a destruction policy, others specify the means of disposal for PII, such as

[37] *See, e.g.*, 16 C.F.R. §§ 314.3(a)-(b) (2012).

[38] 29 C.F.R. § 825.500(g) (2013).

[39] § 1630.14(b)–(d).

[40] § 1635.9(a)(1).

[41] § 1904.29(b)(10).

[42] *See* 201 MASS. CODE REGS. 17.03–17.04 (2013).

[43] *See, e.g.*, ALASKA STAT. § 45.48.530 (2012); COLO. REV. STAT. § 6-1-713(1) (2013); HAW. REV. STAT. § 487R-2(a) (LexisNexis Supp. 2012); N.C. GEN. STAT. § 75-64(b) (2013); OR. REV. STAT. § 646A.622(1) (West 2011).

shredding of hardcopy documents, effective erasure of electronic media, or other actions to render the PII unreadable or indecipherable.[44]

[18] Second, various federal and state laws mandate security breach notification. Under the Health Information Technology for Economic and Clinical Health Act ("HITECH"), covered entities and their business associates must make required notifications if the security or privacy of protected health information ("PHI") is compromised through acquisition, access, use, or disclosure in a manner not permitted under the HIPAA Privacy Rules.[45] State law commonly requires organizations possessing PII of states' residents to notify such residents if there is a breach of security regarding their PII.[46] Virtually every state (except Alabama, Kentucky, New Mexico, and South Dakota) has such a law, and the Texas law implicitly requires that persons conducting business in Texas must also provide breach notification for residents of states that do not have their own breach notification laws.[47]

[19] Third, privacy laws commonly require organizations possessing protected information to provide notification to the affected individuals of the organization's privacy policies for protection of such information, often with related requirements for opt-out or consent regarding information-related practices and transactions. For example, HIPAA covered entities and business associates must comply with privacy standards covering, among other matters, privacy policies and disclosure

[44] *See, e.g.*, CAL. CIV. CODE § 1798.81 (West Supp. 2014); KY. REV. STATE. ANN. § 365.725 (LexisNexis 2008).

[45] *See* 45 C.F.R. § 164.400-164.404 (2012).

[46] *See, e.g.*, GINA STEVENS, CONG. RESEARCH SERV., R42475, DATA SECURITY BREACH NOTIFICATION LAWS 4 (2012) (citations omitted).

[47] *See* TEX. BUS. & COM. CODE ANN. § 521.053 (West Supp. 2013).

consent.[48] Regulations under the Gramm-Leach-Bliley Act mandate that financial institutions provide customers notice of their privacy policies regarding the protection of customer information, and also include requirements for opt-out notifications and mechanisms.[49]

[20] Privacy and data security obligations can also be imposed by contract. For example, an organization may be contractually required to comply with the Payment Card Industry (PCI) Data Security Standard.[50] The PCI Data Security Standard provides technical and operational requirements to protect cardholder data, and it "applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data."[51]

D. Intellectual Property

[21] The law of intellectual property encompasses protection of information in the form of trade secrets, patented inventions, trademarks,

[48] *See* 45 C.F.R. pt. 164, subpt. E.

[49] *See, e.g.*, 16 C.F.R. § 313.4, .7, .9 (2012).

[50] PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES 7 (Version 2.0 ed. 2010) [hereinafter PCI 2.0], *available at* https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

[51] *Id.* at 5. While Version 2.0 of PCI DSS remains active until December 31, 2014, Version 3.0 was issued in November 2013 by the PCI Security Standards Council to allow organizations time to adjust their practices for compliance with the revised requirements. *See* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD AND PAYMENT APPLICATION DATA SECURITY STANDARD: VERSION 3.0 CHANGE HIGHLIGHTS, at 1-2 (2013) *available at* https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf.

and copyrighted works. Trade secret status can exist for "all forms and types of financial, business, scientific, technical, economic, or engineering information" if such information has actual or potential economic value by being neither generally known to, nor readily accessible through proper means, by the public, provided that the information owner has taken reasonable measures to keep such information secret.[52] For example, the court in *Optos, Inc. v. Topcon Medical Systems, Inc.* concluded that the plaintiff could likely establish that its customer information had trade secret status, because the plaintiff required all employees to sign confidentiality agreements, and it also password-protected its computers and limited internal access to information on the customer list.[53]

[22] Organizations seeking patent protection for an invention must be cautious about public disclosures of the invention prior to the filing of the patent application. Organizations can obtain patent protection in the United States if they file a patent application within one year from the date of the invention's first public disclosure.[54] In many foreign patent jurisdictions, however, a public disclosure immediately becomes part of the applicable prior art, thereby precluding patent protection.[55] Disclosures made to contractors, investors, customers, testing labs, or other third parties under a nondisclosure or confidentiality agreement are often not treated as public disclosures that would preclude subsequent

[52] 18 U.S.C. § 1839(3) (2012); *see* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939) (listing factors to be considered in determining whether information is a trade secret, including the extent to which the information is known outside of the business, the extent to which it is known by employees and others involved in the business, and the extent of measures taken to guard the secrecy of the information).

[53] Optos, Inc. v. Topcon Med. Sys., 777 F. Supp. 2d 217, 240 (D. Mass. 2011).

[54] *See* 35 U.S.C. § 102(b) (Supp. 2012).

[55] *See, e.g.*, European Patent Convention, art. 54, Nov. 29, 2000, *available at* http://www.epo.org/law-practice/legal-texts/html/epc/2010/e/ar54.html.

patent protection, as long as there is no commercial exploitation of the invention.[56]

[23] While establishing and maintaining trademark rights simply requires use of the distinctive trademark on goods or services in commerce,[57] the trademark owner must enforce its rights against uses likely to cause customer confusion, and failure to do so risks erosion or loss of enforceable trademark rights.[58] Trademark rights can be lost if the use of the mark becomes generic to describe a type of product.[59] Organizations can also lose trademark protection by allowing third parties to use the trademark with either inadequate quality control provisions or naked licensing, in which there are no limitations or restrictions on the use of the trademark or the quality of goods or services offered under the mark.[60]

[24] Copyrights generally vest in the author of the work,[61] but works produced by the organization's employees are considered works made for hire and, absent an express agreement otherwise, the copyright in such work is owned by the employer.[62] Works of independent contractors,

[56] *See, e.g.*, Invitrogen Corp. v. Biocrest Mfg., 424 F.3d 1374, 1382 (Fed. Cir. 2005) (citations omitted).

[57] *See, e.g.*, Bluebell, Inc. v. Farah Mfg. Co., 508 F.2d 1260, 1265 (5th Cir. 1975).

[58] *See, e.g.*, Herman Miller, Inc. v. Palazzetti Imps. & Exps., Inc., 270 F.3d 298, 317 (6th Cir. 2001).

[59] *See* AmCan Enters., Inc. v. Renzi, 32 F. 3d 233, 234 (7th Cir. 1994) (noting that "'yellow pages' has become a generic term for a local business telephone directory alphabetized by product or service").

[60] *See* Dawn Donut Co. v. Hart's Food Stores, Inc., 267 F. 2d 358, 366-67 (2d Cir. 1959).

[61] *See* 17 U.S.C. § 201(a) (2012).

[62] §§ 101, 201(b).

however, are generally not works made for hire.[63] Thus, organizations must be diligent in contracting for copyrighted works to ensure proper designation as a work made for hire, or, alternatively, to obtain an assignment of copyrights. Organizations must also avoid infringing on third parties' exclusive rights by copying, preparing derivative works, distributing, or publicly displaying or performing the protected works of others without the express permission of the copyright owner.[64]

E. Litigation Preservation

[25] Organizations have a duty to preserve documents and other information that they know or reasonably should know may be relevant to imminent or pending litigation.[65] As stated in *Zubulake v. UBS Warburg, LLC*, "[o]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."[66]

[26] The litigation preservation duty is not found solely in case law. It is also the corollary to statutes and regulations imposing sanctions for destruction of evidence.[67] In addition, numerous statutes and regulations

[63] The definition of "work made for hire" in § 101 includes specific categories of works of independent contractors that are specially ordered or commissioned for use, and that by written agreement may be considered a work made for hire. *See* § 101.

[64] *See* § 106 (listing exclusive rights in copyrighted works).

[65] *See* United States *ex rel.* Koch v. Koch Indus. Inc., 197 F.R.D. 463, 482 (N.D. Okla. 1998).

[66] Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

[67] For example, Section 802 of the Sarbanes Oxley Act provides:

> Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation

explicitly require the preservation of specified information pertinent to governmental proceedings or other litigation.[68]

> or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or in contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

18 U.S.C. § 1519 (2012).

[68] As an example, Equal Employment Opportunity Commission regulations provide that

> [w]here a charge of discrimination has been filed, or an action brought by the Commission or the Attorney General, against an employer under title VII . . . the respondent employer shall preserve all personnel records relevant to the charge or action until final disposition of the charge or action.

29 C.F.R. § 1602.14 (2013). A similar preservation requirement applies to federal contractors. Obligations of Contractors and Subcontractors, 65 Fed. Reg. 68042 (Nov. 13, 2000) (codified at 41 C.F.R. pt. 60) (with text omitted from 41 C.F.R. § 60-1.12(a)); 41 C.F.R. §§ 60-250.80(a), 60-741.80(a) (2013). Many states have a similar preservation requirement for such personnel records. *See, e.g.*, CAL. CODE REGS. tit. 2, § 11013(c)(4) (2014). Organizations in various regulated industries have explicit statutory or regulatory preservation requirements in the context of governmental proceedings or civil litigation. For example, power and gas utilities and their holding companies are required by Federal Energy Regulatory Commission regulations to retain all records relevant to pending litigation, complaint procedures, or government proceedings. 18 C.F.R. §§ 125.2(l), 225.2(l) 368.2(l) (2013). Various regulated activities or operations of general organizations can trigger statutory or regulatory preservation requirements. For example, required records under Equal Credit Opportunity Act regulations must be retained by creditors who have notice of an investigation or enforcement action until final disposition of the matter. 12 C.F.R. §§ 1002.12(b)(4), (6) (2012). Yet violation of a records retention statute or regulation does not necessarily establish sanctionable spoliation:

> [U]nder some circumstances, [a records retention] regulation can create the requisite obligation to retain records, even if litigation involving the records is not reasonably foreseeable. For such a duty to attach, however, the party seeking the inference must be a member of the

[27] The scope of the preservation duty continues to evolve, shaped by case law[69] and rulemaking,[70] and influenced by commentators.[71] Regardless, satisfying the preservation duty is not a passive undertaking.

> general class of persons that the regulatory agency sought to protect in promulgating the rule.

Byrnie v. Town of Cromwell Bd. of Educ., 243 F.3d 93, 109 (2d Cir. 2001).

[69] An early, broad statement of the preservation duty can be found in *William T. Thompson Co. v. General Nutrition Corp.*:

> Sanctions may be imposed against a litigant who is on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence, and destroys such documents and information. While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.

593 F. Supp. 1443, 1455 (C.D. Cal. 1984) (citations omitted). Subsequent case law has established limitations upon this broad scope. *See, e.g.*, Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) ("As a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation.").

[70] Pending amendments to the Federal Rules of Civil Procedure would redefine the scope of permissible discovery in terms of proportionality. If adopted, such a revision of Rule 26 regarding the scope of discovery may well have a symmetrical impact upon the scope of the preservation duty. *See* Zubulake, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (tying scope of preservation duty to the scope of discovery permissible under FED. R. CIV. P. 26(b)(1)).

[71] *See, e.g.*, The Sedona Conference, *The Sedona Conference Commentary on Preservation, Management and Identification of Sources of Information that Are Not Reasonably Accessible*, 10 SEDONA CONF. J. 281, 291-92 (2009) (offering an early proposal for directly applying proportionality to the scope of the preservation duty).

Rather, "[t]he obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers."[72] As a result, the preservation duty is a crucially significant compliance requirement for organizations with pending or impending litigation.[73]

III. LEGAL REQUIREMENTS FOR CORE INFORMATION GOVERNANCE ELEMENTS

[28] It is of course sensible, when designing an information governance program, for an organization to assess its information-related practices, requirements, risks, and opportunities, thereby determining its objectives for information governance.[74] Similarly, it is not surprising that organizations should then implement an information governance program to meet such objectives by developing frameworks and controls for information (Structure), by establishing appropriate policies, procedures, and contractual arrangements, and by providing guidance and training (collectively, Direction), by dedicating roles and responsibilities and providing technology tools and systems (Resources), and by measuring outcomes and providing appropriate consequences for success or failure in

[72] *In re* Prudential Ins. Co. Sales Practices Litig., 169 F.R.D. 598, 615 (D.N.J. 1997).

[73] This article distinguishes between information legal requirements and event-based risks and exposures. Certainly, the preservation duty can be viewed as an obligation triggered by an event or circumstance, namely, a pending or impending lawsuit or governmental proceeding. However, litigation is ubiquitous in the real-world environment of most organizations, and therefore, in this article the fundamental obligation to preserve documents, electronically stored information, and tangible things is treated as a legal requirement.

[74] *See* THE SEDONA CONFERENCE, *supra* note 1, at ii ("The strategic objectives of an organization's Information Governance program should be based upon a comprehensive assessment of information-related practices, requirements, risks, and opportunities.").

meeting expectations and objectives (Accountability).[75] But these key building blocks of Assessment, Structure, Direction, Resources, and Accountability, crucial for defining and establishing an information governance program, are not merely good practice.[76] A variety of laws expressly require organizations to take these steps.[77]

[75] *See id.* ("An Information Governance program should be established with the structure, direction, resources, and accountability to provide reasonable assurance that the program's objectives will be achieved.").

[76] Various standards provide organizations guidance on assessing information practices and providing structure, direction, resources, and accountability for information governance. International Standard ISO 15489-1, *Records Management*, provides a design and implementation methodology for records systems that includes preliminary investigation, analysis of business activity, identification of records requirements, and assessment of existing systems. INT'L ORG. FOR STANDARDIZATION, ISO 15489-1, INFORMATION AND DOCUMENTATION—RECORDS MANAGEMENT § 8.4 (2001). It also addresses the need for records classification and indexing, *see id*. at §§ 9.5.2, 9.5.4, a records management policy and training, *see id.* at §§ 6.2,11, and responsibility and accountability for records management, *id.* at § 6.3.

International Standard ISO 30301, *Management Systems for Records*, requires that organizations establishing records management systems take into account all relevant external and internal factors, business and legal requirements, and related risks and opportunities. INT'L ORG. FOR STANDARDIZATION , 30301, MANAGEMENT SYSTEM FOR RECORDS §§ 4, 6 (2011). The Standard also addresses the importance of the form and structure in which records are created and captured, *see id.* at § 8.2(c)(1)(iii); a records policy and training, *see id.* at §§ 5.2, 7.3; top management's responsibility to provide necessary resources, *see id*. at § 7.1; and accountability through performance evaluation, *see id.* at § 9.

International Standard ISO/IEC 27001, *Information Security Management Systems*, requires organizations establishing an information security management system to identify and assess information security risks. INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM'N, ISO/IEC 27001, INFORMATION SECURITY MANAGEMENT SYSTEMS § 4.2.1 (2005). The Standard also addresses the importance of asset management, including inventory and classification, *see id.* at app. A.7; risk treatment plans, procedures, and training programs, *see id.* at §§ 4.2.2, 5.2.2; the provision of necessary resources, *id.* at 5.2.1; and accountability through periodic audits and reviews, *see id.* at § 4.2.3(d), (e).

A. Legal Requirements for Information Governance Assessments

[29] The majority of legal requirements mandating information-related assessments appear in privacy and data security laws requiring safeguards for protected information.

[30] HIPAA covered entities and business associates must "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."[78] Covered entities and business associates are also required to periodically perform a technical and nontechnical evaluation that establishes the extent to which their security policies and procedures meet the requirements of the HIPAA Security Standards.[79]

[31] Entities governed by the Gramm-Leach-Bliley Act and subject to the FTC Safeguard's Rule must "develop, implement, and maintain a comprehensive information security program" to protect the security and confidentiality of customer information.[80] In developing the mandated

---

For a discussion by ARMA International enumerating generally accepted recordkeeping principles, see *The Generally Accepted Recordkeeping Principles*, ARMA INT'L, http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles (last visited Jan. 15, 2014).

[77] *See infra* Part III.A-E.

[78] 45 C.F.R. § 164.308(a)(1)(ii)(A) (2013).

[79] *See* § 164.308(a)(8).

[80] 16 C.F.R. § 314.3(a)-b (2012). Safeguards requirements under the Gramm-Leach-Bliley Act are also found in rules of the federal functional regulators for various specific types of financial institutions. *See, e.g.*, 12 C.F.R. pt. 30 app. B (pertaining to national banks); 12 C.F.R. pt. 170 app. B. (pertaining to federal savings associations); 12 C.F.R.

information security program, such entities must conduct a risk assessment to "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information . . . and assess the sufficiency of any safeguards in place to control these risks."[81] They must also periodically evaluate and adjust the program in light of testing results, material changes to operations or business arrangements, or other circumstances with a material impact upon the security program.[82]

[32] Financial institutions and creditors subject to the Fair Credit Reporting Act and the FTC's Red Flags Rule that offer or maintain covered accounts "must develop and implement a written Identity Theft Prevention Program . . . designed to detect, prevent, and mitigate identity theft . . . ."[83] Such entities must periodically conduct a risk assessment[84] and must ensure that the resulting program is periodically updated to reflect changes in risks of identity theft.[85]

---

pt. 208 app. D-2 (pertaining to state-chartered Federal Reserve member banks); 12 C.F.R. pt.225 app. F. (pertaining to bank holding companies); 12 C.F.R. pt. 364 app. B (pertaining to federally insured state nonmember banks); 17 C.F.R. § 160.30 (pertaining to commodities dealers); 17 C.F.R. § 248.30 (pertaining to brokers, dealers, investment companies, and investment advisers).

[81] 16 C.F.R. § 314.4(b).

[82] *See* § 314.4(e).

[83] § 681.1(d)(1). Red Flags Rule requirements under the Fair Credit Reporting Act are also found in rules of the federal functional regulators for various specific types of financial institutions. *See, e.g.*, 12 C.F.R. § 41.90 (regulating national banks); 12 C.F.R. § 171.90 (regulating federal savings associations); 12 C.F.R. § 222.90 (regulating state-chartered Federal Reserve member banks); 12 C.F.R. § 334.90 (regulating federally insured state nonmember banks); 17 C.F.R. § 162.30 (regulating commodities dealers); 17 C.F.R. § 248.201 (regulating brokers, dealers, investment companies, and investment advisers).

[84] *See* 16 C.F.R. § 681.1(c).

[85] *See* § 681.1(d)(2)(iv).

[33] Various states require persons or businesses possessing protected personal information of state residents ("PII") to maintain reasonable security procedures and practices to protect such PII from unauthorized use or disclosure. Massachusetts requires such persons and businesses to maintain a written comprehensive information security program, which must include the identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of PII, as well as periodically evaluating and improving the current safeguards' effectiveness.[86] Under Oregon law, mandated information security programs are deemed compliant if they include the identification of reasonably foreseeable internal and external risks to the security of PII and assessment of safeguards sufficiency.[87]

[34] Entities subject by contract to the PCI Data Security Standard must have an annual process to identify threats and vulnerabilities to the security of protected cardholder data, resulting in a formal risk assessment.[88]

B. Legal Requirements for Information Governance Structure

[35] Organizations pursuing information governance need a classification structure or other framework for their information types. Such a framework accurately reflects the different categories of the organization's information, and within the framework the information categories are connected with applicable information governance rules and controls.[89] A familiar example of such a framework is a records retention

[86] *See* 201 MASS. CODE REGS. 17.03(2)(b) (2013).

[87] OR. REV. STAT. ANN. § 646A.622(2)(d)(A)(ii)-(iii) (West 2011).

[88] *See* PCI 2.0, *supra* note 50, at 64; *accord* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES 97 (Version 3.0 ed. 2013) [hereinafter PCI 3.0], *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

schedule, which lists record series (information categories) and, for each record series, a retention period (associated rules). Another example is a data security grid, which lists categories of information organized by security sensitivity, such as confidential, private, and public (information categories), and for each security category, applicable safeguards for security and data protection (associated rules).[90] Intellectual property inventories also can be viewed as information frameworks. Yet another example is mapping of the organization's existing legal holds, showing the footprint or scope of all pending legal holds, with information on the scope and status of each hold.[91] In an information governance program, these frameworks are elements of the overall structure for governing the organization's information.[92]

[36] Various legal requirements compel organizations to establish structures and frameworks for their information. In some regulated industries, organizations are explicitly required to maintain records management classification structures. For example, power and gas utilities and their holding companies must arrange, file, and index their required records to ensure ready identification and access for regulatory

[89] *Cf.* 18 C.F.R. § 125.2(j) (2013) (requiring public utilities regulated by the Federal Energy Regulatory Commission to categorize and arrange information).

[90] *See generally* Reagan Moore, *Back to Basics: What Is a Data Grid?*, INT'L SCI. GRID THIS WK. (June 6, 2012), http://www.isgtw.org/feature/back-basics-what-data-grid; *Record Retention Schedule*, BUS. DICTIONARY, www.businessdictionary.com/definition/record-retention-schedule.html (last visited Jan. 15, 2014).

[91] *See generally* THE SEDONA CONFERENCE, *supra* note 1, at 15.

[92] It has been suggested that organizations can combine these frameworks, particularly records retention schedules and data security grids, into a unified Information Governance Matrix in which all of the organization's information can be classified, allowing all applicable information governance controls and rules to be easily identified. *See* THE SEDONA CONFERENCE, *supra* note 1, at 12.

inspection,[93] and motor carriers must maintain records indexes.[94] Electronic recordkeeping laws commonly require effective systems for arranging and indexing electronic data so that required records can be reliably located, accessed, and retrieved.[95] Also, entities subject to the PCI Data Security Standard must determine and document the scope of their cardholder data environment by identifying all locations and flows of protected cardholder data.[96]

C. Legal Requirements for Information Governance Direction

[37] To accomplish information governance, organizations need to tell people what to do, and also what not to do, regarding the organization's information. Traditional vehicles for such direction include an organization's policies and procedures, its contracts with third parties, and training delivered to employees and other involved personnel.

[93] 18 C.F.R. §§ 125.2(j), 225.2(j), 368.2(d) (2013).

[94] 49 C.F.R. pt. 379, app. A, at M.1 (2012).

[95] *See, e.g.*, DEP'T OF THE TREASURY, INTERNAL REVENUE SERV., REV. PROC. 97-22 § 4.01(5) (1997) (requiring that taxpayers imaging required hardcopy tax records maintain complete descriptions of the related indexing system); 8 C.F.R. § 274a.2(e)(5) (2012) (requiring that employers retaining I-9 documentation in electronic format maintain complete descriptions of the indexing system utilized); 17 C.F.R. § 240.17a-4(f)(3)(vi) (2013) (requiring that securities brokers and dealers maintain indexes for required information maintained in electronic storage media); 29 C.F.R. §§ 2520.107-1(b)(2), 4000.53(b) (2013) (noting that indexing capability is required in electronic recordkeeping systems for benefits records); 48 C.F.R. § 4.703(c)(2) (2012) (requiring that federal contractors imaging records to electronic form maintain effective indexing systems).

[96] PCI 2.0, *supra* note 50, at 10; *accord* PCI 3.0, *supra* note 88, at 10.

1. Policies

[38] Numerous laws explicitly require organizations to have policies or protocols related to the proper handling of information. One such topic is electronic recordkeeping. Thus, employers that opt to complete or retain I-9 forms electronically must maintain documentation of their business processes for creating, modifying, and maintaining the electronic I-9 forms and for establishing their authenticity and integrity.[97] Electronic recordkeeping systems for records required under ERISA must have reasonable controls to "ensure the integrity, accuracy, authenticity and reliability" of such electronic records, including procedures for proper labeling of such records and a quality insurance program.[98] Federal contractors that image required records must have established procedures to ensure the accuracy, reliability, and security of the electronic recordkeeping.[99]

[39] Another such topic is privacy and security for protected information. Thus, HIPAA covered entities and business associates must implement written "policies and procedures to prevent, detect, contain, and correct [ePHI] security violations" in compliance with the HIPAA Security Standards, and also policies and procedures to ensure compliance with the HIPAA Privacy Standards and breach notification rules for PHI.[100]

[40] Entities subject to the FTC's Standards for Safeguarding Customer Information under the Gramm-Leach-Bliley Act must establish a comprehensive information security program that contains appropriate

[97] 8 C.F.R. § 274a.2(f)(1).

[98] 29 C.F.R. § 2520.107-1(b)(1), (5).

[99] 48 C.F.R. § 4.703(c)(1) (2012).

[100] 45 C.F.R. § 164.308(a)(1)(i); *see* §§ 164.316(a), 164.530(i)-(j).

administrative, technical, and physical safeguards for the protection of customer information.[101]

[41] Financial institutions and creditors subject to the FTC's Red Flags Rule under the Fair Credit Reporting Act must develop and implement an Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with opening or maintaining covered accounts.[102]

[42] Several states require persons in businesses possessing PII of state residents to maintain reasonable security procedures to protect such information from unauthorized use or disclosure.[103] Massachusetts requires such persons and businesses to have a written comprehensive information security program.[104]

[43] A majority of states have laws requiring entities with PII of state residents to take reasonable measures to protect such information when it is disposed of or discarded. Alaska, Colorado, Hawaii, North Carolina, and Oregon specifically require such entities to have a disposal policy for PII.[105]

---

[101] 16 C.F.R. § 314.3(a) (2012).

[102] § 681.1(d)(1).

[103] *See, e.g.*, ARK. CODE ANN.. § 4-110-104(b) (Supp. 2011); CAL. CIV. CODE § 1798.81.5(b) (West 2009); MD. CODE ANN., COM. LAW § 14-3503(a) (LexisNexis Supp. 2013); NEV. REV. STAT. § 603A.210(1) (LexisNexis Supp. 2010); OR. REV. STAT. ANN. § 646A.622(1), (2) (West 2011); R.I. GEN. LAWS § 11-49.2-2(2) (Supp. 2013); UTAH CODE ANN. § 13-44-201(1) (Supp. 2013).

[104] *See* 201 MASS. CODE REGS. 17.03(1) (2013).

[105] ALASKA STAT. § 45.48.530 (2012); COLO. REV. STAT. § 6-1-713(1) (2013); HAW. REV. STAT. ANN. § 487R-2(b), (d) (LexisNexis Supp. 2012); N.C. GEN. STAT. § 75-64(b) (2013); OR. REV. STAT. ANN. § 646A.622(1) (West 2011).

[44] A majority of states have laws requiring the protection of social security numbers, subject to exceptions for permissible use. Michigan and Texas require persons who possess or obtain social security numbers from their residents to establish a privacy policy for such information.[106]

[45] Entities subject to the PCI Data Security Standard are required to establish a security policy that addresses all PCI DSS requirements, supported by a variety of security procedures, and must review and update the policy whenever the cardholder data environment changes.[107]

2. Third-party Contracts

[46] Federal and state laws contain many requirements for contracts between organizations and third parties that use, store, maintain, process, or dispose of the organization's information.

[47] Laws governing electronic recordkeeping require that contracts and licenses for such electronic generation or storage systems in no way limit or restrict access to and use of such systems by the regulating governmental agency.[108]

[48] Intellectual property law requires third-party nondisclosure agreements to maintain trade secret protection[109] and to avoid public

[106] MICH. COMP. LAWS § 445.84(1) (2004); TEX. BUS. & COM. CODE ANN. § 501.052(a)(1) (West 2009).

[107] PCI 2.0, *supra* note 50, at 64-69; *accord* PCI 3.0, *supra* note 88, at 97-106.

[108] *See, e.g.*, 8 C.F.R. § 274a.2(e)(3) (2012) (discussing the requirements regarding I-9 electronic recordkeeping systems); 29 C.F.R. §§ 2520.107-1(b)(4), 4000.53(d) (2013) (discussing the requirements regarding electronic recordkeeping systems related to ERISA benefits).

[109] *See supra* text accompanying notes 52-55.

disclosures of inventions precluding subsequent patent protection.[110] Trademark law requires that third-party contracts and licenses contain adequate quality control provisions to avoid the loss of enforceable trademark rights.[111]

[49] Under the HIPAA security standards, covered entities may permit business associates to create, receive, maintain, or transmit ePHI on their behalf so long as they obtain satisfactory assurances that such associates will appropriately safeguard the ePHI, with such assurances documented in a written contract.[112] The HIPAA Privacy Standards require business associate agreements ("BAAs") for service provider arrangements involving all protected health information.[113] These requirements extend outward to subcontractor relationships between business associates and their service providers, thereby expanding the applicability of the BAA requirement to any subcontractor that creates, receives, maintains, or transmits ePHI or PHI on behalf of a covered entity's business associate.[114]

[50] Entities subject to the FTC's Safeguards Rule under the Gramm-Leach-Bliley Act must oversee service providers that receive, maintain, process, or otherwise have access to consumer information by providing services to such entities.[115] Such entities are specifically required to take reasonable steps in selecting and retaining such service providers and must

[110] *See supra* text accompanying notes 54-56.

[111] *See supra* text accompanying note 60.

[112] *See* 45 C.F.R. §§ 164.308(b), 164.314 (2012).

[113] §§ 164.502(e), 164.504(e).

[114] *See* §§ 164.308(b)(1), 164.502(e)(1).

[115] *See* 16 C.F.R. §§ 314.2(d), 314.4(d) (2012).

also require, by contract, that the service providers implement and maintain appropriate safeguards.[116]

[51] Financial institutions and creditors subject to the FTC's Red Flags Rule must "[e]xercise appropriate and effective oversight of service provider arrangements," such as by contractually requiring data security safeguards.[117]

[52] The FTC's Disposal Rule requires covered entities to properly dispose of consumer information in order to protect against unauthorized access to or use of such information in connection with its disposal.[118] If such entities use a service provider for records destruction, they must conduct due diligence and contract with, and monitor contract compliance of, the records destruction business to ensure compliant disposal of material containing customer information.[119]

[53] Various states, including California, Maryland, Massachusetts, Nevada, and Rhode Island, require persons and businesses possessing PII of state residents to oversee service providers with access to such PII, including requiring by contract that the service provider establish reasonable security procedures and practices to protect the PII from unauthorized access, destruction, use, modification, or disclosure.[120]

---

[116] §§ 314.4(d)(1), 314.4(d)(2).

[117] § 681.1(e)(4).

[118] *See* § 682.3(a).

[119] *See* § 682.3(b)(3).

[120] *See, e.g.*, CAL. CIV. CODE § 1798.81.5(c) (West 2009); MD. CODE ANN., COM. LAW § 14-3503(b) (LexisNexis Supp. 2013); NEV. REV. STAT. ANN. § 603A.210(2) (LexisNexis Supp. 2010); R.I. GEN. LAWS § 11-49.2-2(3) (Supp. 2013); 201 MASS. CODE REGS. 17.03(2)(f) (2012).

Several states have similar service provider contract requirements specifically for organizations using a records disposal vendor.[121]

[54] Entities subject to the PCI Data Security Standard must manage service providers with which they share cardholder data, including requiring such service providers by contract to acknowledge responsibility for the security of cardholder data they possess, and must also monitor their service providers' PCI DSS compliance status at least annually.[122]

3. Training

[55] A similar variety of federal and state laws mandate effective training on applicable requirements for proper handling of information.

[56] Employers that complete or retain I-9 Forms electronically must implement an effective records security program, including employee training to minimize the risk of unauthorized or accidental alteration or erasure of such electronic records.[123]

[57] HIPAA covered entities and business associates must implement a security awareness and training program for all members of their workforce, including management.[124] The HIPAA Privacy Standards

[121] *See, e.g.*, ALASKA STAT. § 45.48.510(3) (2012); HAW. REV. STAT. ANN. § 487R-2(c) (LexisNexis Supp. 2012); 815 ILL. COMP. STAT. ANN. 530/40(c) (West Supp. 2013); N.C. GEN. STAT. ANN. § 75-64(c) (2013); OR. REV. STAT. ANN. § 646A.622(3) (West 2011); S.C. CODE ANN. § 37-20-190(B) (Supp. 2013).

[122] PCI 2.0, *supra* note 50, at 67-68; *accord* PCI 3.0, *supra* note 88, at 102-104.

[123] *See* 8 C.F.R. § 274a.2(g)(1)(iii) (2012).

[124] *See* 45 C.F.R. § 164.308(a)(5)(i) (2012).

extend this requirement to workforce training regarding privacy and also breach notification compliance requirements.[125]

[58] Entities subject to the FTC Safeguards Rule under the Gramm-Leach-Bliley Act must, as part of their comprehensive information security program, address employee training and management regarding protection of customer information.[126] Financial institutions and creditors subject to the FTC's Red Flags Rule must train staff as necessary to effectively implement their mandated identity theft prevention program.[127]

[59] Several states explicitly require training as an element of required programs for protection of state residents' PII. Thus, Massachusetts requires employee training on the proper use of computer security systems and on the importance of personal information security,[128] and Oregon requires training and management of employees regarding the organization's security program practices and procedures.[129]

[60] Entities subject to the PCI Data Security Standard must implement a formal security awareness program for all personnel on the importance of cardholder data security, with education delivered upon hire and thereafter at least annually, and must also obtain annual acknowledgments that personnel have read and understood the security policy and procedures.[130]

---

[125] *See* § 164.530(b).

[126] *See* 16 C.F.R. § 314.4(b)(1) (2012).

[127] *See* § 681.1(a), (e)(3).

[128] *See* 201 MASS. CODE REGS. 17.04(8) (2013).

[129] *See* OR. REV. STAT. ANN. § 646A.622(2)(d)(A)(iv) (West 2011).

[130] PCI 2.0, *supra* note 50, at 67; *accord* PCI 3.0 *supra* note 88, at 101.

D. Legal Requirements for Information Governance Resources

[61] It is inescapable that organizations establishing an information governance program will need to invest in the initiative by providing resources. Personnel time and effort will be necessary to establish and administer the program, and technology tools and systems will be needed to provide information management and control capabilities. Organizations may also decide to procure outside expertise in the legal, consulting, and technology fields to assist in implementing and sustaining their information governance programs.

[62] Various laws explicitly or implicitly require organizations to provide necessary resources for information governance. First, a variety of laws require the appointment of one or more individuals with dedicated responsibilities regarding information compliance. For example, HIPAA covered entities and business associates must designate a security official who is responsible for developing and implementing the policies and procedures required by the HIPAA Security Standards,[131] as well as a privacy official who is responsible for developing and implementing the policies and procedures required under the HIPAA Privacy Standards.[132] Entities subject to the FTC Safeguards Rule under the Gramm-Leach-Bliley Act must designate one or more employees responsible to coordinate the mandated information security program.[133] Financial institutions and creditors subject to the FTC Red Flags Rule must obtain approval of their initial written identity theft prevention program from either their board of directors or an appropriate board committee, and must subsequently involve the board of directors, an appropriate board committee, or a designated senior management employee in overseeing,

[131] *See* 45 C.F.R. § 164.308(a)(2) (2012).

[132] *See* § 164.530(a)(1)(i).

[133] *See* 16 C.F.R. § 314.4(a) (2012).

developing, implementing, and administering the program.[134] Massachusetts and Oregon require organizations that possess PII of their respective states' residents to designate one or more employees to coordinate and maintain the organization's information security program.[135] In addition, entities subject to the PCI Data Security Standard must assign specified responsibilities for information security management to a designated individual or team.[136]

[63] Second, laws requiring organizations to have certain information system capabilities implicitly require such organizations to provide the resources to have such capabilities. For example, electronic recordkeeping laws requiring such systems to arrange and index electronic data so that required records can be reliably located, accessed, and retrieved[137] compel organizations to invest the resources necessary to comply with such requirements.

[64] Last, laws prescribing that certain information controls be in place[138] or that certain testing or monitoring activities be performed[139]

[134] *See* § 681.1(e)(1)-(2).

[135] *See* OR. REV. STAT. ANN. § 646A.622(2)(d)(A)(i) (West 2011); 201 MASS. CODE REGS. 17.03(2)(a) (2013).

[136] *See* PCI 2.0, *supra* note 50, at 66; *accord* PCI 3.0, *supra* note 88, at 100-101.

[137] *See, e.g.*, *supra* note 95 and accompanying text.

[138] *See, e.g.*, 45 C.F.R. § 164.312 (2012) (requiring HIPAA covered entities and business associates to establish technical safeguards for ePHI, including access control, audit controls, information integrity controls, person or entity authentication controls, and transmission security controls); 201 MASS. CODE REGS. 17.04 (2013) (requiring entities possessing PII of state residents to establish a security system covering their computers, including any wireless system, with secure user authentication protocols, secure access control measures, encryption safeguards, firewall protection, and system security agent software); PCI 3.0, *supra* note 88, at 100-01 (requiring broad range of controls for protected cardholder information).

implicitly require that such organizations devote the resources needed to satisfy such requirements.

E. Legal Requirements for Information Governance Accountability

[65] As with any system of compliance policies and controls, an effective information governance program needs an element of accountability to help ensure that its controls are adhered to and its policies are followed. Information-related legal requirements compel such accountability mechanisms in at least two respects. First, various laws require that organizations designate individuals as responsible for establishing and administering the particular information compliance program,[140] and such individuals are therefore responsible and implicitly accountable for their legally required role on behalf of the organization.[141]

[66] Second, some laws expressly require organizations to take disciplinary action when individuals fail to comply with the particular law's information requirements. Thus, entities possessing PII of

[139] *See, e.g.*, OR. REV. STAT. ANN. § 646A.622(2)(d)(B)-(C) (West 2011) (requiring entities that possess PII of Oregon residents to regularly test and monitor the effectiveness of key technical controls, systems, and procedures); 45 C.F.R. § 164.308 (requiring HIPAA covered entities and business associates to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports); 201 MASS. CODE REGS. 17.04(4) (requiring entities possessing PII of Massachusetts state residents to monitor their computer systems for unauthorized use of or access to personal information); PCI 2.0, *supra* note 50, at 60-62 (requiring vulnerability scans and penetration testing); *accord* PCI 3.0, *supra* note 88, at 91-95.

[140] *See* 16 C.F.R. § 314.4(a) (2012); 45 C.F.R. §§ 164.308(a)(2), 164.530(a)(1); 201 MASS. CODE REGS. 17.03(2)(a); PCI 2.0, *supra* note 50, at 66; *accord* PCI 3.0, *supra* note 88, at 100-101.

[141] *See* 45 C.F.R. § 164.308(a)(2).

Massachusetts residents are required to impose disciplinary measures for violations of the rules of their mandated information security program.[142] HIPAA covered entities and business associates must apply appropriate sanctions against workforce members who fail to comply with the organizations policies and procedures for the security of ePHI and the privacy of PHI.[143] Additionally, covered entities and business associates that know of a pattern of activity or practice of their respective business associates or subcontractors that constitutes a material breach or violation under the applicable business associate contract must terminate the business associate relationship if reasonable steps to cure the breach or end the violation are unsuccessful.[144]

IV. LEGAL REQUIREMENTS WITH INFORMATION GOVERNANCE SYNERGY

[67] As noted above, legal requirements for records retention, electronic recordkeeping, privacy and data security, intellectual property, and litigation preservation do not operate in isolation. Rather, they have interacting repercussions. Such overlaps create synergies for organizations adopting the information governance approach.

[68] Examples of such synergistic areas include gaining clarity on the existence, location, and status of the organization's information;[145] applying information governance controls to information crossing the organization's perimeter;[146] and defensibly disposing of information no

[142] *See* 201 MASS. CODE REGS. 17.03(2)(d).

[143] *See* 45 C.F.R. §§ 164.308(a)(1)(ii)(C),164.530(e)(1).

[144] *See* 45 C.F.R. § 164.504(e)(1)(ii), (2)(iii).

[145] *See infra* Part IV.A.

[146] *See infra* Part IV.B.

longer required for legal compliance or business need.[147] These three examples illustrate the different kinds of synergies useful for reinforcing information governance.

A. Information Clarity

[69] To succeed in governing its information, an organization needs clarity about what information is in its possession or control, the protected or confidential status of the information, the physical location of such information, the format and storage media used for such information throughout its lifecycle, and the identity of the function or role in the organization with stewardship responsibility for the information.[148] Such information clarity is a necessary prerequisite to information governance, for it is not feasible to apply compliance rules, risk controls, and value maximization to information that is off the organization's radar.

[70] This example, information clarity, illustrates synergy by *accumulation*. Legal requirements in each of the various information disciplines work together to compel organizations to obtain such clarity regarding the identity, status, format, location, and stewardship of their information, amplifying the imperative of information clarity.[149] Thus, compliance with records retention legal requirements necessitates clarity about what required records are retained, where they are retained, and who retains them. Similarly, electronic recordkeeping laws require organizations to accurately understand what content is maintained in what permissible media, in what location, and in what systems with prescribed capabilities and controls.[150] A prerequisite to privacy and data security

[147] *See infra* Part IV.C.

[148] *See, e.g.*, 45 C.F.R. §§ 164.306(a), 164.308(a)(2), 164.310(a)(1), 164.312(a)(1).

[149] *See, e.g.*, 45 C.F.R. § 164.306(c).

[150] *See supra* text accompanying note 95. As discussed above, various laws explicitly require index systems for compliant recordkeeping.

compliance is organizational clarity on what information, with what protected status, is located where, and who has access to it.[151] Intellectual property law requires trade secret, invention, trademark, and copyright owners to clearly understand what information, located where, has what protected status, so that such protections for specific information will not be compromised or lost. In addition, the litigation preservation duty compels parties and their attorneys to understand specifically what information is subject to the preservation duty, as well as the location, format, and accessibility of such information.[152]

[71] An organization that has adopted information governance will consider the accumulated impact of these various legal requirements, as well as the related risks and exposures, and as a result will be more motivated to establish efficient and effective information structures and policies yielding greater clarity about its information.

[151] *See, e.g.*, 45 C.F.R. § 164.306(a). This need for clarity regarding information location, status, and format is particularly acute in the circumstance of a security breach of protected information. For example, if an organization suffers the theft of a laptop containing unencrypted personnel data, such as employee names in combination with Social Security numbers, the affected employees will likely need to be notified of the PII security breach pursuant to the law of their residency states. *See, e.g.*, MASS. GEN. LAWS ch. 93H, § 3 (2012); OR. REV. STAT. ANN. § 646A.604(1)-(3) (West 2011). In most such states, if the number of affected individuals exceeds a certain threshold, the organization will also need to notify the state's Attorney General. *See, e.g.*, MASS. GEN. LAWS ch. 93H, §§ 3, 4, 6. If the organization has no reasonable clarity regarding what information, regarding what individuals, was contained in the stolen laptop, it will dramatically magnify the resulting effort, costs, and reputational damage in its breach notifications and remediation for the incident.

[152] *See, e.g.*, Zubulake v. UBS Warburg, LLC, 229 F.R.D. 422, 432 (S.D. N.Y. 2004) ("[C]ounsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture.").

B. Cross-perimeter Controls

[72] In the past, many organizations relied upon their perimeter walls, both physical and virtual, to control their information. While network firewalls and physical boundaries remain useful for certain purposes, the reality is that information flows into and out of organizations more freely now than ever before through such arrangements as service provider relationships and cloud computing.[153] Yet the organization remains subject to applicable records retention, electronic recordkeeping, privacy and data security, intellectual property, and litigation preservation requirements; it is therefore crucial for the organization to understand what of its information is in the custody of others on its behalf and how to properly manage its relationships with such third parties through effective selection, contracting, and oversight.[154]

[73] This example—the need for control of information in third-party arrangements and relationships—demonstrates synergy through *extension*, meaning the use of the more detailed requirements found in one discipline (*i.e.*, privacy and data security) to lead the way for establishing policies, controls, and practices that help with information issues and risks arising under the other disciplines.

[74] Third-party relationships, and the resulting movement of the organization's information beyond its perimeter walls, create risks and exposures regarding records retention, electronic recordkeeping, intellectual property, and litigation preservation. Legal requirements imposing records retention responsibilities are not rendered inapplicable simply because the organization has made arrangements with a third party

[153] *See generally* George B. Delta & Jeffrey H. Matsuura, *§10.02 Controlling Network Access*, *in* CCH LAW OF THE INTERNET, 2013WL3924193 (3d ed. 2013).

[154] *See supra* text accompanying note 95; *see also* 45 C.F.R. §§ 164.306(a), (c), 164.308(b)(1), 164.314(a)(1)-(2).

to perform functions on the organization's behalf.[155] Legal requirements for electronic recordkeeping may explicitly prohibit contracts or licensing that interfere with the organization's obligation to provide information access to the applicable regulatory agency.[156] Intellectual property rights may be diluted or lost if third party relationships do not have sufficient contractual controls.[157] Litigation production duties extend to discoverable information in the responding party's control, despite a lack of possession or custody by such party,[158] and as a result the litigation preservation duty can extend to discoverable documents and data that are solely in the possession of an organization's service provider, nevertheless considered in the organization's control.[159]

[75] Unlike these other information-focused disciplines, privacy and data security laws contain explicit compliance requirements for the management and oversight of third party information relationships. Thus, to satisfy explicit privacy and data security legal requirements, organizations must oversee third parties by conducting due diligence prior

[155] Upon rare occasions, a regulation may explicitly provide for allocation of recordkeeping responsibility between an organization and a service provider for records the organization is otherwise required to be keep. For example, certain records must be kept pursuant to the Federal Trade Commission's Telemarketing Sales rule by the seller or telemarketer, but the regulations allow the seller and its telemarketer to allocate responsibility between themselves for the required recordkeeping by written agreement. *See* 16 C.F.R. § 310.5(c) (2012).

[156] *See supra* text accompanying note 108.

[157] *See supra* Part II.D.

[158] *See* FED. R. CIV. P. 34(a)(1).

[159] *See, e.g.*, Carrillo v. Schneider Logistics, Inc., No. CV 11-8557-CAS (DTBx), 2012 U.S. Dist. LEXIS 146903, at *39 (C.D. Cal. Oct. 5, 2012) (holding that the defendant had ownership over surveillance video tapes with the ability to request them from its third-party security vendor and ordering defendant to produce the tapes after defendant failed to produce surveillance video tapes held by the vendor).

to forming the relationship, by ensuring that third-party contracts contain necessary terms and assurances for information controls, and by effective monitoring of the third party's performance under the contractual relationship.[160]

[76] Organizations applying the information governance approach can use this synergy to strengthen their internal processes for business partner selection, contracting, and contract management, using privacy and data security requirements as their roadmap to establish processes that will also address other information-related risks. Thus, due diligence, contract approvals, and relationship management processes can be modified to more consistently and reliably address third-party records retention, electronic recordkeeping, intellectual property issues, and litigation preservation issues, in addition to privacy and data security mandates. This synergy will thereby better ensure that all of the organization's information governance objectives are met regarding information shared with or held by third parties.

C. Defensible Destruction

[77] In the absence of both a legal retention requirement and an applicable preservation duty, it is by definition legally permissible for an organization to dispose of information in a compliant manner. The reality is, however, that far too many organizations maintain far too much information without any legal requirement or business need to do so.[161]

---

[160] *See supra* text accompanying notes 112-22.

[161] *See, e.g.*, Brian J. Greenberg, *Seven Questions Every CIO Should Be Able to Answer About e-Discovery and Legal Holds*, GEN. SYS. DYNAMICS, http://gsysd.com/articles/what-every-cio-needs-to-know-about-legal-holds.html (last visited Feb. 20, 2104) ("Most organizations turn over far too much information exposing the company to additional legal and financial risk. Freezing everything and keeping all backup data forever is almost never the correct solution to the problem and only creates much larger problems.").

The results of this unfortunate practice include unnecessary storage costs and inefficiencies in the organization's operations, uncertainties arising about the integrity and reliability of information, and exposures to unnecessary litigation expense due to the uncontrolled accumulation of unnecessary information.[162]

[78] This example—addressing the uncontrolled accumulation of unnecessary information—illustrates synergy by *counterbalance*, which is the use of compliance requirements found in one or more of the information disciplines to balance the effect of legal requirements in the other disciplines and thereby to reach the appropriate result.

[79] Neither records retention requirements nor litigation preservation duties compel organizations to dispose of information.[163] Records retention laws in the United States are generally expressed in a "mandatory minimum" manner, in which the statute or regulation requires that the record be retained for a period of time, or for at least a minimum period of time, without a requirement that the record be disposed of at the end of that period.[164] Similarly, the litigation preservation duty, once

[162] *See* THE SEDONA CONF., THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE 1, 6-7, 32, 36 (Charles R. Ragan et al. eds., 2005), *available at* https://thesedonaconference.org/publication/Managing%20Information%20%2526%20Records.

[163] Compliant disposal of information no longer required to be maintained by applicable laws or the organization's policies is a well-accepted records management practice, despite the general absence of a legal requirement in recordkeeping laws to so dispose. *See* INT'L ORG. FOR STANDARDIZATION, ISO 15489-1, INFORMATION AND DOCUMENTATION—RECORDS MANAGEMENT § 7.1(j) (records management programs should ensure "that records are retained only for as long as needed or required"). *See generally Generally Accepted Recordkeeping Principles: Principle of Disposition*, ARMA INT'L, http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles/disposition (last visited Mar. 4, 2014).

triggered, creates an obligation to preserve information within its scope, at least until the duty's existence comes to an end.[165] While case law acknowledges the prerogative of organizations to have and to follow a records retention schedule, such permission comes with the caveat of the preservation duty's mandate to preserve information relevant to pending or impending litigation.[166]

[80] Privacy and data security laws, however, create synergy by providing counterbalance. There cannot be a security breach for information that has previously been disposed of in a legally compliant manner. Therefore, privacy and data security laws requiring the safeguarding of protected information implicitly compel organizations to compliantly dispose of such information once it is no longer needed. Some privacy and data security legal requirements expressly require such disposal. For example, HIPAA business associate contracts must provide that, if feasible, upon contract termination all protected health information received from the covered entity, or created or received on its behalf by the business associate, must be returned or destroyed with the business associate retaining no copies of such information.[167] Furthermore, entities

[164] *See, e.g.*, 47 C.F.R. § 64.604(c)(D)(7) (2012) (providing an example of a mandatory minimum standard in the telecommunication context).

[165] *See generally* Jason A. Phil and Derek E. Larsen-Chaney, *Litigating Litigation Holds: A Survey of Common Law Preservation Duty Triggers*, 17 J. TECH. L. & POL'Y 193, 199-200 (2012) (defining the litigation preservation duty).

[166] *See* Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) (citing Christopher R. Chase, *To Shred or Not to Shred: Document Retention Policies and Federal Obstruction of Justice Statutes*, 8 FORDHAM J. CORP. & FIN. L. 721-23 (2003)) ("'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. . . . It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.").

[167] 45 C.F.R. § 164.504(e)(2)(ii)(I) (2012).

subject to the PCI Data Security Standard must limit data retention time to that required by legal, regulatory, and business requirements.[168]

[81] Intellectual property law also provides a counterbalance. Unnecessary retention of information exacerbates risks of intellectual property loss. For example, trade secret status can be lost through inadvertent public disclosure of information, and the ability to patent an invention can be lost through disclosures occurring prior to patent application filings.[169]

[82] Organizations adopting the information governance approach can fortify their resolve to defensibly dispose of unnecessary and unrequired information by explicitly aligning such efforts with intellectual property protection and privacy and data security compliance.

V. CONCLUSION

[83] Information governance, by its very nature, encompasses more than legal compliance. It is a holistic approach that also addresses information-related risks while optimizing information value. But compliance with legal requirements for records retention, electronic recordkeeping, privacy and data security, intellectual property, and litigation preservation has a crucial role to play. By mandating foundational elements of information governance programs, and through their collective, synergistic interplay, information legal requirements can, and should, be harnessed by organizations to make effective information governance a reality.

[168] PCI 2.0, *supra* note 50, at 28; *accord* PCI 3.0, *supra* note 88, at 34.

[169] *See supra* text accompanying notes 52-56.