By Charles H. Kennedy, Partner, Wilkinson, Barker, and Knauer LLP

SECURE RECORDS DISPOSAL: IS *NOT* SHREDDING EVER A GOOD IDEA?

Contents

Businesses have a choice of records disposal methods. Where paper records are concerned, businesses might put those records in the trash, turn them over to a recycling company, or use a more secure method such as burning or shredding.

In choosing among these disposal methods, companies typically weigh cost, convenience, business risk and legal risk.

The legal risks of different disposal methods can be the hardest factors to assess. The state and federal statutes and regulations that affect the choice of disposal methods are varied and complex. With that in mind, this paper describes the laws and regulations that businesses should keep in mind before choosing one disposal method over another, and explains why any decision that involves insecure disposal of any group of paper records should be made only after the most careful consideration.

In U.S. law, secure disposal is required when a record contains personally identifiable information (PII).[1] This generally includes any information, such as a name, address, telephone number, email address, Social Security number or other data, that can be used to identify an individual person.

I. When Is Secure Disposal Required?

In U.S. law, secure disposal is required when a record contains personally identifiable information (PII).[1] This generally includes any information, such as a name, address, telephone number, email address, Social Security number or other data, that can be used to identify an individual person.

The state and federal statutes and regulations that require secure disposal of records containing PII fall into many categories, but the most important are state secure disposal ("must shred") laws, state data security laws, and state and federal data protection laws related to particular industries and activities. The following looks at each of these categories in turn.

A. THE STATE "MUST-SHRED" LAWS

Most states now have statutes that require organizations maintaining PII to take reasonable measures to dispose of those records in a secure fashion[2]. California's statutory language is typical:

Organizations that maintain records containing personal information should be aware of several features of these secure disposal laws.

A business shall take reasonable steps to destroy, or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.[3]

First, these state laws require companies to dispose properly of records containing the personal information of those states' residents, regardless of where the companies are incorporated and regardless of whether those companies have permanent employees and facilities in those states. So, if an organization has customers in any of the majority of states with secure disposal laws, that organization must comply with those states' secure disposal requirements.

[1] We use "PII" here as a useful generic term, but individual privacy laws often use different terms, such as "personal information," "individually identifiable information," "non-public personal financial information," and other expressions to identify the data those laws protect. What all of these laws have in common is their application to data about individual persons.

[2] *See* A.R.S. § 44-7601; A.C.A. § 4-110-104; Cal. Civ. Code § 1798.81; C.R.S. § 6-1-713(1); O.C.G.A. § 10-15-2; KRS § 365.725; MCL § 445.72; NJ Stat. § 56:8-162; NY CLS Gen. Bus. § 399-h; N.C. Gen. Stat. § 75.64; Tenn. Code Ann. § 39-14-150(g); Tex. Bus. & Com. Code § 48.102; V.S.A. § 2445; Rev. Code Wash. § 19.215.010; Wis. Stat. § 895.505.

[3] Cal. Civ. Code § 1798.81.

Second, unless a company plans to set up different, parallel methods of records destruction for customers who reside in different states, that company will have no choice but to use a method that satisfies the requirements of the state with the most rigorous statute. Where paper records are concerned, that method is shredding.

Specifically, nearly all of the secure disposal laws specify three possible methods of records disposal: shredding, erasure of personal information, and modification of the record to make the personal information illegible. The second and third methods are useable only with electronic media, which can reliably be erased, overwritten or encrypted. The fact that a few states, such as North Carolina, permit burning or pulverizing as alternatives to shredding is relevant only if all of a company's customers live in one of those few states. Otherwise, shredding is the only option that ensures nationwide compliance.

Finally, some, but not all, of the secure disposal laws require companies to exercise due diligence in selecting a records disposal vendor.

Finally, some, but not all, of the secure disposal laws require companies to exercise due diligence in selecting a records disposal vendor. For example, North Carolina requires a business entering into a written contract with a records destruction vendor to exercise "due diligence" in selecting that vendor, which might include review of an independent audit, checking references, or reviewing the vendor's policies and procedures.[4] In the event of a data loss caused by a vendor's negligence, this requirement might make a company liable for failure to base its choice of a vendor on solid evidence of reliability. Accordingly, a company that has customers in any of the states that impose a due diligence obligation must be prepared to demonstrate that it selected its records disposal vendor with appropriate care.

[4] N.C. Gen. Stat. § 75.64(b).

B. STATE DATA SECURITY LAWS

A number of states have enacted laws that go beyond secure disposal obligations, and require businesses to protect PII throughout the life cycle of the records containing that information, including at the time of disposal.[5]

These comprehensive data protection laws effectively mandate compliance with all of the technical, physical and administrative "best practice" measures by which responsible companies protect personal information from unauthorized access, disposal and use. Those measures might range from antivirus software and firewalls, to employee security training, to secure records storage and control of physical access to premises where personal information is maintained. Those measures also include secure disposal of records that have reached the end of their life cycle and usefulness to the business.

C. STATE SECURITY BREACH NOTIFICATION LAWS

Nearly all states now have enacted statutes that require businesses maintaining PII to notify affected persons when the security of records containing that information has been compromised.[6] The language of California's law, which was the first such statute to be adopted, is typical:

Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[7]

Some features of these security breach notification statutes are especially worth noting.

Some features of these security breach notification statutes are especially worth noting.

First, businesses should be aware that under many of the applicable laws, security breaches must be reported, even when there is no solid evidence that an incident has resulted in identity theft or other harm to individuals.

Second, because state breach notification laws now protect well over 90% of the nation's population, very few businesses can avoid reporting of data breaches simply because no such law has been enacted in their states of

[5] *See* A.C.A. § 4-110-104; Cal. Civ. Code § 1798.81; Nev. Rev. Stat. § 603A.210; R.I. Gen. Law § 11-49.2-2; Tex. Bus. & Com. Code § 48.102; Utah Code Ann. § 13-44-201.

[6] *See* A.C.A. § 4-110-105; Cal. Civ. Code § 1798.82(a); Conn. Gen. Stat. § 36a-701; 6 Del. C. § 102(a); Fla. Stat. § 817.5681; O.C.G.A. § 10-1-912; Haw. Rev. Stat. § 487N-2: Idaho Code § 28-51-105; 815 ILCS 530/10(a); La. R. S. § 51:3074; Minn. Stat. § 13.055; Mont. Code Anno. § 30-14-1704; N.J. Stat. § 56:8-163; NY CLS Gen. Bus. § 899-aa; N.C. Gen. Stat. § 75-65; N.D. Cent. Code § 51-30-02; ORC Ann. § 1347.12; R.I. Gen. Laws § 1-49.2; Tex. Bus. & Com. Code § 48.103(b); 9 V.S.A. § 2435(6); Rev. Code Wash. § 19.255.010; Wis. Stat. § 895.507.

[7] Cal. Civ. Code § 1798.82(a).

A company that failed to report a breach of the security of personal information, simply because that information was maintained in paper rather than digital form, would invite adverse publicity and scrutiny from state and federal regulators.

incorporation or principal states of operation. A company with affected customers in any state with a breach notification law effectively must advise those customers of reportable incidents. Having done so, the company cannot prudently fail to give a similar report to all affected persons in every state, including states that might lack breach notification laws. To discriminate in reporting depending upon customers' states of residence almost certainly would invite enforcement actions by the Federal Trade Commission (FTC) and state attorneys general.

Finally, businesses should not be misled by the fact that most breach notification statutes cover only unencrypted *computerized* information. For one thing, this limitation is not true of all the states' laws. North Carolina, for example, requires a business "that owns or licenses personal information in any form (whether computerized, paper, or otherwise) [to] provide notice to the affected person that there has been a security breach following discovery or notification of the breach."[8] Accordingly, a company that has even one North Carolina customer is required to report a breach of personal information concerning that customer, regardless of the form in which the information is maintained.

More fundamentally, a company that failed to report a breach of the security of personal information, simply because that information was maintained in paper rather than digital form, would invite adverse publicity and scrutiny from state and federal regulators. Such a failure to report, if sufficiently publicized, also would encourage state and federal legislators to adopt statues that specifically require reporting of breaches involving paper records.

[8] N.C. Gen. Stat. § 75-65(a).

D. SECTOR-SPECIFIC FEDERAL LAWS

The U.S. still does not have a comprehensive, federal data protection law that requires companies in all sectors of the economy to maintain and dispose of records containing PII in a secure fashion (although this may change soon). However, a number of federal laws and regulations require secure storage and disposal of records that include certain categories of PII, or that are generated in the course of certain activities.

One such statute is the Gramm-Leach-Bliley Act, which protects the privacy of individuals' non-public financial information.[9] As implemented by regulations of the FTC and the various banking regulatory agencies, the Gramm-Leach-Bliley Act requires all financial institutions to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [the institution's] size and complexity, the nature and scope of [the institution's] activities, and the sensitivity of any customer information at issue."[10] The required program must address "information processing, storage, transmission and disposal."[11]

Another important federal statute is the Health Insurance Portability and Accountability Act (HIPAA) which protects the privacy of personal health information.[12] Like the Gramm-Leach-Bliley Act, HIPAA and the implementing regulations of the Department of Health and Human Services require covered entities to develop and implement administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of personal information covered by the statute. The required programs must protect covered data at all stages of its life cycle, including disposal.

Another significant federal statute, and one that specifically imposes secure disposal obligations, is the Fair and Accurate Credit Transactions Act (FACTA).[13] The disposal obligations of FACTA are implemented by the FTC's Disposal Rule, which expressly requires companies maintaining information derived from credit reports to dispose of that information in a secure fashion, and to exercise due diligence in the selection of records disposal vendors.[14]

Finally, although the U.S. lacks a federal-level law that requires protection of personal data across all sectors of the economy, the FTC has taken on a leading role as the protector of individual privacy. In that capacity, the FTC has brought many enforcements against companies that failed to protect personal information, including companies that failed to dispose of paper records in a secure fashion.[15] The FTC has brought these proceedings under its broad authority to regulate "unfair or deceptive acts or practices," and a number of companies have entered into lengthy consent decrees, and paid substantial financial penalties, for failures to protect personal information.

[9] Gramm-Leach-Bliley Financial Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999).
[10] 16 CFR § 314.1.
[11] 16 CFR § 314.1.
[12] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[13] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 111 Stat. 1952 (2003).
[14] 16 CFR § 682.3(a).

II. So, When Is Shredding Optional?

We have described the legal framework within which a business's decision to shred, or not to shred, particular documents must be made. What does this framework tell us?.

We have described the legal framework within which a business's decision to shred, or not to shred, particular documents must be made. What does this framework tell us?

First, *any* paper record that contains personal information about any individual should be disposed of in a secure fashion. Even if a company is not a financial institution subject to Gramm-Leach-Bliley or a health care company subject to HIPAA, it almost certainly is subject to the FTC's jurisdiction and to multiple state breach notification, data security or secure disposal laws. All of those statutes, and the implementing regulations, protect the security of the personal information of individuals. Any personal information an organization collects will be subject to multiple such laws and regulations.

How does a company determine which paper records are most likely to contain personal information subject to these various statues and regulations? The obvious places to begin are the records of the Marketing Department, which contain contact and account information of customers, and the records of the Human Resources Department, which contain the employment records of company personnel. Shredding of all records generated by those departments is a prudent first step toward compliance with applicable state and federal laws.

[15] *See,* e.g., FTC Press Release, "Company Will Pay $50,000 Penalty for Tossing Consumers' Credit Report Information in Unsecured Dumpster," http://www.ftc.gov/opa/2007/12/aumort.shtm.

Businesses also must be aware of any work processes that might cause personal information to "migrate" from place to place within an organization.

Does this mean that disposal of records in other departments can safely be left to the discretion of individual personnel, or simply addressed by throwing records in the trash or turning them over to insecure recycling services?

This approach might be prudent if it can safely be assumed that other departments will not generate or store information about individuals. However, the basis for such an assumption should be closely examined. For example, the fact that an employee does not work in Human Resources does not mean that the employee never gains access to employee records; similarly, the fact that an employee does not work in Marketing does not mean that the employee never gains access to customer records. Depending upon how computer system access privileges are assigned and maintained, employees may acquire, review and print out sensitive information far removed from their normal responsibilities. Reduced to printouts and other physical media, that information might be stored and disposed of insecurely, with responsible managers unaware of its existence until a security incident occurs.

Businesses also must be aware of any work processes that might cause personal information to "migrate" from place to place within an organization. For example, a merchant that engages in mail order or online marketing might keep customer contact information, not just in the sales department, but also in the departments that arrange for shipping of orders. Similarly, customers' credit card information might initially be acquired and used by the sales or order fulfillment departments, but might afterwards be stored in a central computer to which all employees have access, and from which printouts can be generated at any work station.

None of this means that *all* companies must dispose of *all* paper records by shredding. It does, however, suggest that when a business acquires and stores personal information at any point in the organization, it must consider the possibility that that information will reappear at every other point in the organization. As with so many processes, the secure records storage and disposal chain is only as strong as its weakest link.

IRON MOUNTAIN®

ABOUT IRON MOUNTAIN. Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company Web site at www.ironmountain.com for more information.