RECORD RETENTION, THE PANDEMIC, AND THE NEW REMOTE WORK ENVIRONMENT: IS YOUR BUSINESS AT RISK?

BRANDI L. DONIERE is the Co-Chair of the Litigation & Information Management Practice Group at Brouse McDowell, LPA and practices primarily in the areas of information governance and litigation management. In Brandi's information governance practice, she helps companies develop and implement document retention and information usage policies, audit information practices, identify and preserve information for potential litigation, and assess litigation readiness. In her litigation management practice, Brandi coordinates discovery nationally for a major manufacturer as part of a national product liability discovery team. In addition to her litigation and information management practices, Brandi also has experience recovering insurance proceeds for policyholders and litigating business and consumer rights lawsuits in both state and federal courts. Brandi is a member of the Electronic Discovery Institute.

MARGUERITE E. ZINZ, the Co-Chair of the Litigation & Information Management Practice Group at Brouse McDowell, LPA, concentrates her practice in the areas of information governance and litigation management. Marguerite helps businesses in developing and auditing record retention and information governance policies and in the defensible disposition of information. She also assists clients in a variety of litigation readiness endeavors, including identifying key people and information sources and establishing protocols and procedures for protecting a company's trade secrets, both internally and during litigation. As national discovery counsel for a major manufacturer, Marguerite coordinates discovery nationally in products liability litigation. Marguerite has also assisted in the restructuring of a national network of defense counsel and worked with clients and other counsel on larger scale document collection and review projects.

The 2020 pandemic profoundly impacted society, forcing many of us to change the way we shop, learn, socialize, exercise, worship, and work. Some of the most significant changes have been to the workplace and the way work is done. Rather than reporting to an office each day, many employees learned to work effectively and productively from home using various forms of technology. Supervisors became adept at managing projects remotely and presiding over meetings virtually. Large conferences were replaced with live and on-demand video presentations that allow attendance without travel. And many of these changes were made on very short notice as states quickly imposed gathering restrictions. Information technology professionals have never worked harder to keep organizations going. All should be applauded for their ability to adapt during uncertain times. But have these necessary changes put your business at risk when it comes to record retention? Now that the work-from-home model is becoming more of the rule than the exception, what does that mean for your organization's record retention policies?

Record retention is generally not top of mind for most organizations and often does not generate the same sense of urgency as other business interests. In a world where time and money are limited, record retention can be viewed as nonessential, even superfluous. Employees' compliance is often presumed or taken for granted. But record retention issues, if left unchecked, can lead to increased operational and litigation risks that can ultimately be quite costly to an organization's bottom line and reputation. And, unfortunately, the pandemic-induced remote work environment has made these risks even more likely.

WHAT IS A RECORD RETENTION POLICY?

A record retention policy can have many names–document retention policy, information governance policy, information management policy, and

recordkeeping policy to name a few. Whatever it is called, at its core, a record retention policy provides an overall plan for an organization's records and information governance program by instructing employees how to handle information that is generated or used in the course of business. It also helps a business navigate and reduce operational and litigation risks by appropriately protecting the organization's records and proprietary information. At a minimum, an effective record retention policy should: (1) define key terms, including what constitutes a record and disposable information; (2) explain key concepts, like legal holds; and (3) identify information that should be retained and for how long.

A record retention policy does not stand alone. For instance, record categories and retention periods for each category are generally outlined in a record retention schedule that is separate from the record retention policy. Likewise, a business may have a separate, more detailed legal hold policy. Record management procedures, like instructions for document management systems, naming conventions, and procedures for storing and disposing of records, may also all be outlined in separate documents. Other policies that may come into play when considering an organization's entire records and information governance program include: computer/acceptable use policies, personal device/BYOD policies, information security policies, social media policies, data privacy policies, and trade secret policies.

WHY IS RECORD RETENTION IMPORTANT?

A business operates more efficiently when its records are consistently handled in accordance with a record retention policy and a records and information governance program that are tailored to the organization's needs. The efficiencies come from the ability to locate records quickly and the confidence that the records are accurate and up to date. When the same records are stored in multiple locations instead of their designated place, it can take longer to find them or ascertain whether a given record is the most current version. Efficiency is also furthered by appropriately disposing of records that are no longer needed for business purposes and for which preservation is not required due to a legal hold. By properly reducing the records an organization possesses in accordance with an effective record retention policy, businesses can easily locate important and necessary information.

Consistent compliance with the policies and procedures of a tailored record retention policy and a records and information governance program provides numerous other benefits to an organization, often best measured by the costs that are avoided.

Protection of valuable confidential and proprietary information

The success of a business often depends on its ability to maintain the confidentiality of its trade secret and other proprietary information. If guidelines for creating, accessing, storing, and using records are ignored, or if information is retained longer than necessary, the risk increases that confidential information will be accessed by, or disclosed to, an unauthorized party or competitor, whether inadvertently or intentionally. Depending on the nature of the information disclosed, the result to an organization could be quite damaging, even catastrophic. Businesses such as the Coca-Cola Company, Kentucky Fried Chicken, McDonald's, and the maker of WD-40 would have faced greater competition and certainly suffered lower sales had they been unable to maintain the secrecy of the ingredients in their flagship products. A smaller company could be devastated if a competitor learned the identities of its customers and sales tactics and used that knowledge to lure business from the company.

The safeguarding and proper dispositioning of protected third party information

New privacy laws, like the General Data Protection Regulation (GDPR) in Europe, are being adopted in more and more states. As they become more commonplace, businesses need to ensure that their information management practices meet the new requirements and are being properly followed or they could face substantial fines. For instance, the GDPR establishes the general policy that personal data should only be retained as long as required for

the legitimate purpose for which it was gathered.[1] Personal data is defined quite broadly to include any information that relates to an identified or identifiable person.[2] This would include obvious items such as names, physical and email addresses, and phone numbers, as well as items such as IP addresses or cookie identifiers. Serious violations of the GDPR's requirements to protect this information could result in fines up to €20 million, or four percent of the organization's worldwide annual revenue from the previous year, whichever is higher.[3] For less severe violations, the fines are up to €10million or two percent of the organization's revenue.[4] These types of fines are not just a slap on the wrist. But an effective and properly implemented record retention policy and records and information governance program that address applicable privacy laws can easily avoid them.

Assurance that regulatory requirements are met

In addition to privacy laws, there are many other government regulations that mandate specific retention periods for certain categories of information. For example, the Occupational Safety and Health Administration (OSHA) requires businesses with 11 or more employees to retain logs of work-related injuries and illnesses for at least five years.[5] The Employee Retirement Income Security Act (ERISA) similarly requires organizations that administer an employee benefit plan to retain any records that must be disclosed under that plan for six years from the date on which they were required to be disclosed.[6] Regulatory retention requirements can also include provisions regarding how particular information must be maintained—and failing to comply with these requirements can be quite costly. Abercrombie & Fitch, for instance, was fined $1,047,110 by the Office of Homeland Security Investigations after a 2008 Form I-9 inspection revealed record-keeping deficiencies in its I-9 verification system.[7] The Financial Industry Regulatory Authority (FINRA) has also issued fines of over $1 million for failing to maintain electronic records in a format that prevents alteration, as required by Security and Exchange Commission (SEC) regulations.[8] A record retention policy tailored to the business can readily address any applicable regulations, likely through a record retention schedule that notes such laws along with the retention periods or other requirements prescribed for specific categories of information.

Assurance that contractual obligations are met

Business contracts may set out requirements regarding certain information exchanged or generated because of the contract. Provisions of a contract could require, for example, that a business partner's information be stored in a certain manner, in a secure location, and returned or deleted after a designated time. Failure to honor these obligations could subject an organization to a breach of contract claim and potentially business tort claims. Once again, such claims can be avoided with a record retention policy that encompasses all the organization's legal obligations, both those prescribed by statute or regulation and those that arise via contractual commitments.

Potentially reduced litigation costs

The discovery phase of litigation is notoriously costly. When records that are potentially relevant to the claims and defenses in a lawsuit are not properly stored in their designated places and instead are found in multiple locations, whether in physical warehouses and filing cabinets or on servers, hard drives, and other devices, locating those records to respond to discovery requests will inevitably take longer and cost far more than if proper procedures are followed under an effective record retention policy. Additionally, if a business fails to dispose of information in accordance with its policies and retains records beyond either their usefulness or any retention obligation, a much larger pool of information is left to be collected, searched, reviewed, and produced if relevant. Each of these steps adds even more cost to what already may be a very costly process.

Evidence of reasonableness if retention practices are ever challenged

When information that is potentially relevant in a lawsuit no longer exists, an organization may face spoliation claims. As long as the information was

dispositioned prior to the anticipation of litigation, the existence of, and compliance with, a written record retention policy and records and information governance program may serve as key evidence that destruction of the information was reasonable and not done in bad faith. "[C]ourts ... ordinarily do not draw an inference of bad faith when documents are destroyed under a routine policy."[9] For example, in a lawsuit alleging that a property management company had violated the Fair Credit Reporting Act, plaintiffs accused the company of spoliating evidence by burning lease applications and credit reports. The company was able to establish that it regularly destroyed such records to prevent inadvertent disclosure of third parties' private information. Even though some relevant records may have been destroyed after the company became obligated to retain them, the court held that there was no evidence of bad faith, as the records were destroyed pursuant to the company's reasonable record retention policy.[10]

Protection of reputation and goodwill

An organization does not want to be viewed as an untrustworthy business partner. Nor does any business want to become newsworthy because of a data or information breach that results in the loss of its customers' and employees' personal information or the loss of its trade secrets and other proprietary information. Bad publicity can lead to decreased sales and lower stock values, both of which are good indicators of damaged reputation and goodwill. According to a recent study conducted by technology research company Comparitech, data breaches have an overall negative effect on share price.[11] Comparitech looked at eight publicly-held technology companies that suffered data breaches and found that before the breaches, the companies' stock prices significantly outperformed the NASDAQ and that six months after the breaches, their stock values had dropped an average of three percent below the NASDAQ.[12] These changes in stock prices are not insignificant. An effective and properly implemented record retention policy and records and information governance program can help an organization avoid data and information breaches that could cause substantial loss in sales or stock value.

HOW HAS THE PANDEMIC IMPACTED RECORD RETENTION?

Record retention practices were undoubtedly affected by the sudden shift of office staff from a centralized, in-person office to a remote, work-from-home environment. Many organizations were ill-prepared for an all-remote workforce, resulting in employees using their personal devices to conduct business from home. Business records may have been duplicated for ease of use and could now exist in multiple places, including on personal devices outside the organization's control and security protocols. Records that are created or updated outside business systems may not make it back to their approved location within the organization where they can be retained in accordance with the organization's record retention policy and records and information governance program. Without adequate security protections, personal devices are also highly vulnerable to security breaches.

For many organizations, working from home was made possible only by adopting various forms of new technologies, including use of video conferencing platforms, channel-based messaging platforms, and ephemeral messaging applications. Each of these technologies presents its own set of record retention challenges likely not contemplated by existing record retention policies and records and information governance programs.

Video conferencing platforms

In-person meetings were replaced with virtual video conferences on a large scale, with Zoom being the most popular service provider. Zoom and other video conferencing platforms allow users to share their screens, which could inadvertently reveal sensitive information to persons not authorized to see such information. Zoom also allows users to record and save recordings of virtual meetings through the platform. Depending on the subject matter of the meeting, the recording is potentially a record that is required to be retained under the record retention policy. And, even if not a record under the policy, the recording may be subject to a litigation hold, depending on its subject matter. These are all

possible records that did not exist, at least not in this potential volume, before the pandemic.

Channel-based messaging platforms

Channel-based messaging platforms, such as Microsoft Teams, Slack, and Google Hangouts, allow users to create different channels for projects or user groups. Users of a particular channel can share files with and send messages to other users belonging to the channel. While certainly efficient, messaging platforms potentially present issues similar to video conferencing. What may have previously been an in-person discussion is now recorded in messaging on the platform and may constitute a record. Depending on the platform and the nature of the account the organization has with the platform, a business may also have difficulty readily obtaining information that is needed for litigation or other purposes. Further, if channels are not monitored and limited to those individuals required for the specific project or issue, protection of confidential information may also be a concern.

Ephemeral messaging applications

Ephemeral messaging applications, such as Snapchat, WhatsApp, Confide, and Wickr, are yet another means of communicating that have increased in use throughout the pandemic. These types of applications include two important and distinctive features: (1) automated disposition/deletion of the message from the applications of both the sender and the recipient; and (2) end-to-end encryption. Used properly, ephemeral messaging can benefit an organization's record retention efforts by facilitating compliance with privacy laws like the GDPR and by automatically eliminating voluminous data that has no ongoing business value, such as routine communications and meeting requests. Despite these benefits, an organization should be mindful of the legal and regulatory risks of using of ephemeral messaging if the information that is being shared is information that should be retained under the organization's record retention policy.

Individual departments within a business will also likely have their own unique record retention issues because of the pandemic. For example, Human Resources departments were necessarily required to spend a good amount of time on tasks pertaining to sick leave and preventing the spread of COVID-19 infections. This did not mean their other duties stopped or that more personnel were added to the department. Instead, HR professionals balanced these new, time-consuming tasks with all their prior responsibilities, including furloughing employees, transferring job duties to different positions or personnel, and recruiting, hiring, and training new employees. With all these extra duties and stresses, it would not be surprising if certain record retention procedures were overlooked. Exit procedures for the transfer of records and processing of computers may not have been followed, potentially resulting in the loss of information that is required to be retained under the record retention policy. Likewise, with limited time and resources, training of new employees regarding the record retention policy and records and information governance program may have taken a back seat to training on other, more essential business functions. While the risks from lack of training are not necessarily immediate, lack of training could result in the mishandling of records or the loss of information the organization needs or is legally required to retain.

WHAT CAN AN ORGANIZATION DO TO MITIGATE ITS RECORD RETENTION RISKS?

With many organizations and employees realizing the benefits of a more remote workforce, it appears that many of the newly adopted work practices and technologies are here to stay. Businesses should evaluate these new practices and technologies and either adopt new record retention policies and procedures to address them or revise existing policies. In doing so, organizations should be mindful of the potential risks and costs associated with the new practices and technologies and attempt to minimize them where appropriate. In conjunction with these revisions, an organization should:

1. Survey employees on their current record retention practices, including identification of specific technology, how the identified technology

is being used, and any storage locations. The survey will help the business identify areas that need to be addressed in the revisions to its record retention policy and records and information governance program. It will also guide the organization to areas in which employees may need additional or refresher training and may identify specific pandemic-related or work-from-home retention issues.

2. Audit employee compliance with the record retention policy and the records and information governance program. The audits can focus on general employee awareness of the record retention policies and procedures or reviewing actual practices. Audits on individual practices will identify specific record retention issues resulting from the remote work environment. And like the survey, audits can also help identify areas in the record retention policy and records and information governance program that need revision and highlight items requiring additional training.
3. Train employees on the revised record retention policies and procedures and on any items identified via the survey or audit. Any missed training for new employees should also be conducted, emphasizing not only the record retention policy and schedule but also any additional records management procedures, like instructions for document management systems, naming conventions, and any other storage or disposal requirements.
4. Correct and mitigate any specific record retention issues arising from the sudden switch to a remote work environment identified during the survey or audit. If an issue cannot be mitigated and important information is lost, the organization should document the issue and all the steps taken to locate and retrieve the information. Having a written record of what happened and what was done to attempt to mitigate will help if the business is required to defend itself regarding the missing records in litigation or before regulatory agencies.
5. Consider engaging an outside records and information governance professional to guide mitigation efforts and evaluate existing policies or draft new policies. Hiring legal counsel will provide additional evidence of good faith and reasonableness when an organization's record retention practices are contested. Businesses that have a weak record retention history or anticipate future challenges to records handling and information governance decisions would also benefit from the support of a legal professional.

Much like many of the hardships felt from the pandemic, the impacts of the global crisis and the quick change to a remote work environment on record retention can feel quite daunting to navigate. The good news is that it is not too late and the sooner your business acts the better. By embracing the steps identified above, your organization can identify any potential areas of concern and greatly reduce the risk of records-related penalties and operational losses.

Notes

1 General Data Protection Regulation 2016/679, art. 5 (1)(e), 2016 O.J. (L 119) (EU).

2 Id., at art. 4 (1).

3 Id., at art. 83 (5).

4 Id., at art. 83 (4).

5 29 C.F.R. § 1904 et seq.

6 29 U.S.C.A. § 107.

7 Press Release, U.S. Immigr. and Customs Enf't, Abercrombie & Fitch fines after I-9 audit (Sep. 28, 2010) (www.ice.gov/pi/nr/1009/100928detroit.htm).

8 Press Release, FINRA, FINRA fines 12 Firms a Total of $14.4 Million for Failing to Protect Records From Alteration (Dec. 21, 2016) (www.finra.org/media-center/news-releases/2016/finra-fines-12-firms-total-144-million-failing-protet-records).

9 Pipes v. United Parcel Serv., Inc., No. 07-1762, 2009 U.S. Dist. LEXIS 62942 at *4 (W.D. La. 2009).

10 Martinez v. Triple S Properties, 2018 WL 4658700 (W.D. Missouri 2018).

11 Paul Bischoff, How Data Breaches Affect Stock Market Share Prices, Comparitech, Feb. 9, 2021, available at https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/.

12 Id.