HOARDERS BEWARE:

Defensible Data Disposal Is Good Business

By Pamela C. Williams and John D. Martin

Data disposal can be a highly sensitive topic. Spoliation of evidence carries great risks and penalties, including reputational, civil and even criminal. Today, corporations are producing data at astounding rates. This new business reality exacerbates challenges associated with legacy data issues, including questions about how to properly manage data that may be stored on antiquated media types or that is no longer readable. Maintaining data beyond legal requirements and business needs is risky and expensive, driving up litigation costs and slowing response time when companies are faced with litigation and forced to review and address data that was stored unnecessarily.

As trusted advisors, in-house counsel are called upon to provide guidance to clients on these issues. In-house counsel are also targets: When litigation or discovery goes bad, defensibility of their approach can be called into question. The ever-changing legal landscape can make navigating the maze of global and jurisdictional requirements complex.

30-SECOND SUMMARY

This article tees up issues to consider in making the internal business case for resources to design, guide and implement defensible disposal practices, and practical considerations and steps to take in implementing these practices. In addition, the article suggests considerations about information governance and lifecycle issues going forward, and value-add to the business and legal department resulting from implementing sound defensible disposal practices.

A defined workflow process, strategic planning, thorough documentation, and clearly defined roles and responsibilities are all important elements of implementing a defensible disposal practice. The first step involves forming a team. In assembling the core team, consider including representatives from legal, IT, records management and business units. Members of this team should have knowledge of corporate policies, programs, systems, processes and records management practices, and should have relationships with outside vendors who may store or manage the company's data.

The next step of implementing a defensible disposal practice involves assessing current practices and requirements; be sure to determine whether there are any special circumstances that may need to be taken into account with regard to certain data sets. Finally, develop a project management plan.

The business case for including defensible disposal within good information governance practices

If disposing of data is risky business, then why not just keep everything? Simply put: It just does not make good business sense to keep everything beyond legal requirements and business needs. It is also risky to keep everything. Further, it is expensive, and with the exponential increase in data creation, the time is now ripe to revisit corporate information governance practices and how defensible disposal fits in.

However, implementing a thoughtful and defensible approach requires buy-in at the top levels of the company, involving the right people to help chart and implement the path forward, and time and resources. Following are some factors to consider in making the business case to incorporate defensible disposal practices into a company's business information lifecycle/data stewardship practices.

Some eye-opening statistics

A recent Compliance, Governance and Oversight Council reference guide lists some impressive factors:

- Ninety percent of the data in the world was created in the past two years.
- For most organizations, information volume doubles every 18–24 months.
- In a typical company in 2011, storing data consumed about 10 percent of the IT budget.
- At a growth rate of 40 percent, storing data will consume over 20 percent of the typical IT budget by 2014.
- Most companies have failed to dispose of unnecessary data accumulated over the past decade.
- CIOs everywhere are shedding costs and reducing IT spend as a percentage of revenue.

Add to this, challenges with existing data that is:

- stored on media types where required software or hardware may no longer be available to read the data;
- unlabeled (including data in hard copy boxes, CDs, flash drives, tapes, etc.);
- on media types that may have deteriorated; and/or
- acquired as part of an acquisition, while the people familiar with the data are no longer with the company or have forgotten the processes.

Compound all of this with the fact that maintaining data is no longer needed for legal or business purposes:

- *adds risks* — especially if inconsistent with records management policies and practices;
- *is expensive* to store and maintain;
- *makes litigation preparedness and response time more cumbersome and lengthy* — decreasing efficiency and increasing litigation costs; and
- *makes discovery more expensive* — increasing costs to review a much larger data set than may have been necessary.

The solution is defensible disposal practices

With buy-in from top management secured, what are some of the practical steps to get started in implementing practices to defensibly dispose of data that is not required to be retained for legal or business purposes? What steps can companies consider taking to integrate defensible disposal practices within a company's overall electronic information management practice plan?

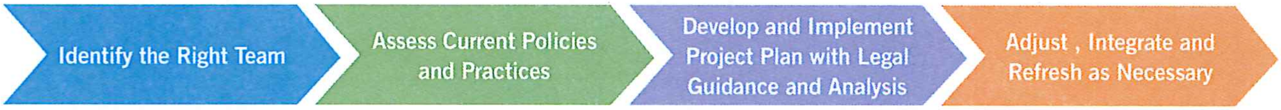
As an initial step, consider whether the company would like to undertake the defensible disposal project under the direction of counsel as part of an overall review of corporate records and information management systems, programs and practices. Key next steps to consider are listed below.

Identify the right team

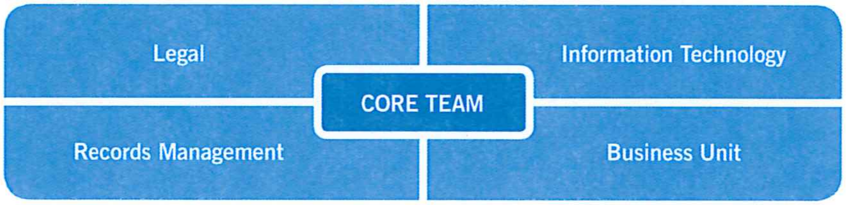
Be collaborative, and include team members with knowledge of the company's data, systems, policies, business

Pamela C. Williams is vice president and counsel for WellPoint, Inc. Williams and her team are responsible for corporate litigation and related activities affecting thirteen of the fourteen Blue Cross and/or Blue Cross/Blue Shield plans that WellPoint operates. *pam.williams@anthem.com*

John D. Martin is a partner at Nelson Mullins Riley & Scarborough LLP. Martin leads the firm's Electronic Discovery Practice Group and its Encompass Information Governance and Discovery Services Division. *john.martin@nelsonmullins.com*


Identify the Right Team
Assess Current Policies and Practices
Develop and Implement Project Plan with Legal Guidance and Analysis
Adjust , Integrate and Refresh as Necessary

Identify the right team



practices and legal requirements. Documenting steps taken is critical to a defensible plan, so also consider who will be on point for developing and maintaining documentation to track key steps and decision points in connection with executing the plan. Consider whether including external counsel would be helpful to guide overall strategic approach, to provide advice on legal hold and retention requirements, and to advise on process defensibility.

In assembling the core team, consider including representatives from legal, IT, records management and business units with knowledge of:

- organizational structure;
- corporate policies, programs, systems, processes and records management practices;
- relationships with outside vendors who may store or manage the company's data; and
- legal requirements and litigation/ investigative hold process.

Assess current practices and requirements

Begin by considering applicable legal requirements, including identifying what legal requirements and guidelines might inform defensible disposal practice considerations.

If the company has a centralized approach to records management and/ or legal holds, identify and assess how any existing policies address managing data or records that are no longer subject to retention requirements or to litigation or investigative holds.

In addition, determine whether there are any special circumstances that may need to be taken into account in connection with the implementation and data analysis phases (see below), including whether a litigation or investigation imposes a duty to preserve every copy of a document, or whether any opposing or third-party agreements impose special requirements with regard to certain data sets.

Develop and implement a project management plan

A defined workflow process, strategic planning, thorough documentation, and clearly defined roles and responsibilities are important elements of the overall approach.

- **Documenting the project:** Consider creating a project map or plan that identifies key workflow steps, beginning with planning and data inventory of potential data or media types in need of remediation, and extending through legal analysis, disposition and documentation. Think about how legal holds and guidelines for sampling and review fit into the overall workflow. In addition to documenting the upfront plan and key project guidelines, ensure that the overall approach includes documenting the disposition decision and the supporting legal analysis, being mindful of potential privilege and waiver implications.
- **Planning and inventory:** In addition to defining the project scope and resources, identify and categorize populations of data. Are there categories of data that can be easily excluded from the defensible disposal analysis — because the material clearly is or is not subject to legal holds or other retention requirements? For other categories of data potentially subject to analysis, inventory and define the data categories based on available information. In addition, as part of the inventory process, gather any additional relevant information that may be available (e.g., for decommissioned servers, include information on the type of system, the type of data on the servers, whether data was migrated to another system, whether data is accessible, who is responsible, etc.).

ASSESS EXISTING POLICIES AND PRACTICES. QUESTIONS TO CONSIDER INCLUDE:

- What legal requirements and guidelines might inform defensible disposal practice considerations?
- When were current litigation/ investigative hold policies implemented?
- How do the policies treat backup media?
- How do the policies treat duplicate data?
- Are there current or former technology vendors with responsibilities in connection with maintaining corporate data and records?
- If yes, what types of data and records do they have and what do any agreements say?

DOCUMENTATION CONSIDERATIONS INCLUDE:

- What are the key steps in the process?
- What are the data types subject to review?
- What legal holds are active and what are the date ranges?
- Are there attorney–client privilege issues to consider in the structuring approach?

PLANNING AND INVENTORY CONSIDERATIONS INCLUDE:

- What is the project scope?
- Who are the key players on the core team?
- What are the various data populations? Can any be excluded?
- What information is available on data populations subject to analysis?

IMPLEMENTATION CONSIDERATIONS INCLUDE:

- Are there factors (such as data source, dates and nature of data) that might exclude the data as not being subject to a legal duty to preserve, regulatory retention requirement or having continuing business value?
- Is the same data stored elsewhere?
- Will sampling or technical analysis be conducted?
- Are sampling or testing guidelines needed?
- Will data be migrated or sent to a third party for further analysis?
- Will outside technology vendors be used? What are the guidelines and contract issues?

- **Implementation:** Building upon the foundation established in strategically mapping the project workflow, analyze the data and the applicability of legal, retention and business requirements.

  Considerations include:
  - *Sole data source:* Does the data duplicate data stored elsewhere or is it the sole data source? To the extent it duplicates data stored elsewhere, it may not need to be preserved.
  - *Analysis of data sources:* In reviewing data sources, factors to consider include whether the data source can be read, the age and origin of the data source, volume and purpose (e.g., whether the data is back-up data captured solely for the purpose of disaster recovery restoration or whether it is stored for archival purposes), etc.
  - *Sampling:* If the data source is unknown, and other factors don't otherwise clearly exclude it from further consideration, would sampling be helpful to assess the contents to help determine whether they are likely relevant or if they can be disposed? If yes, consider how sampling should occur, what types of guidelines and protocols are necessary, initial criteria for sampling, etc.
  - *Data repository:* If data will be sent to an off-site repository for analysis, consider requirements for any off-site vendors to receive the data, process for migrating the data, whether data will be encrypted, process for encrypting data and process for data that cannot be encrypted, and provisions to include in vendor agreements.
  - *Legal requirements and guidelines:* Analyze legal requirements and guidelines, including litigation holds and preservation requirements, regulatory retention requirements and corporate policies.

- **Disposition:** Documentation during this step is key; include thorough documentation of the steps taken, information considered and analysis conducted to arrive at a decision whether or not to dispose of data. If it is determined that data may be disposed, consider appropriate steps to properly dispose of the data, including any information security or privacy considerations, and document those steps and the date and method of disposal.

Preventive practices: Information governance

As companies consider and refresh various corporate governance and compliance practices, prospective attention to information governance makes good sense. For example, identifying personnel, technology, business-process and business-structure changes that might occur, and considering how information and data associated with these changes should be treated, can help better position a company to integrate good information governance practices into everyday business practices. Considering these issues upfront could help reduce the creation of large volumes of unnecessary data and, perhaps, even the need for defensible disposal efforts down the road. It could also help increase the likelihood that information lifecycle issues are systematically addressed and help enhance overall corporate information management and litigation readiness practices.

Timing can be an issue — deciding to embrace new, wholesale information governance practices in the midst of a large litigation or corporate crisis could be scrutinized as suspect. However, when the time is right, undertaking a well-reasoned assessment of current information governance policies and taking systematic steps to enhance existing practices, where needed, can bring value to the company.

Some issues to consider in connection with information governance practices going forward include:

- *Records and information management policies and practices:* Do policies clearly articulate requirements in connection with retention, preservation and disposal? How are these requirements communicated and to whom? Is training part of the rollout? Are there reminders or refreshers along the way?

- *Electronic communications and social media:* Does the company have policies relating to electronic communications and social media? What do they say regarding business and/or personal use? How do they address use of electronic communications and/or social media for business purposes, as well as access to and management of that information?
- *Litigation holds:* What happens when litigation holds are lifted? How is that phase of the information hold lifecycle addressed in policies and practices?
- *Unknown data types:* Are there systematic practices that can be implemented to help reduce creation and accumulation of unknown data?
- *People changes:* As people move within the company or leave, what types of practices are in place to handle employee information? Do HR policies and practices integrate with overall records and information management policies and practices? What steps do IT and corporate security take to help address information management when employees transfer within the company or leave?
- *New systems and technology, including the cloud:* As companies migrate from old systems and embrace new technology, what happens to data from prior systems? Will new systems bring new data types? What types of changes to policies and processes may be required to address new ways of working?
- *Bring your own device:* How do corporate policies address BYOD and business data on personal devices? Are there systems and policies in place to help ensure that data does not uniquely reside on personal devices? What happens when employees with BYOD access to company systems leave or send their devices in for repair, trade in for an upgrade or lose the device?
- *Technology and records management vendor changes:* Consider what happens when making a change from an existing vendor and what types of provisions should be included in agreements with new vendors. What do agreements say about retention, access to and return of information, usability of information after the relationship ends, any back-up information and disposal or retrieval?
- *Acquisitions, joint ventures and divestitures:* What types of policies and practices are in place to address how corporate information will be managed in connection with new corporate structures or changes? For acquisitions, how will new systems and records and information management policies and practices be integrated? How will litigation holds relating to litigation from acquired companies be managed? For divestitures, what happens to corporate information for the company that is being divested? What are the preservation, retention and disposal considerations? For joint ventures, how will information be managed? What policies and practices will apply, and which laws (e.g., foreign jurisdictions) apply to those ventures?
- *Working smarter and automating:* Are there features of existing or new technology that might automate and build in business and legal rules consistent with records management policies and requirements? How do these features integrate with overall systems, and what types of considerations need to be addressed to help adjust when people, business, technology or legal changes come into play?

Companies with defensible practices in place enhance their litigation position.

ADJUST, INTEGRATE AND REFRESH: SYSTEMATIC INTEGRATION

Consider the following in assessing information governance practices going forward:

- records and information
- policies and practices
- electronic communications and social media
- litigation holds
- unknown data types
- people changes
- new systems and technology
- BYOD (Bring Your Own Device)
- vendor changes
- acquisitions, joint ventures and divestitures
- working smarter and automating

Value for the corporate client

If implementing defensible disposal practices requires an up-front investment in resources (including people, time and perhaps technology) to achieve desired results, what is the anticipated return on investment? Why is this important? Potential value-add for the corporate client includes:

- *Reduces risks:* Properly managing information that is no longer needed for legal or business purposes helps reduce the company's corporate risk profile. Systematically addressing upfront how the company will manage

ACC EXTRAS ON... Record management

ACC Docket
Can Your Records Management Program Handle Ediscovery? (May 2011).
www.acc.com/docket/rmp-ediscovery_may11

Presentations
How to Design a Legally Defensible Records Retention Plan (Oct. 2011).
www.acc.com/defensible-records_oct11

Leveraging Technology to Defensibly Manage Electronic Records (Oct. 2012).
www.acc.com/manage-records_oct12

InfoPak^{SM}
Effective Records Management (Sept. 2012).
www.acc.com/infopaks/rm-8issues_sep09

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

information that is eligible for disposal, and documenting steps taken to demonstrate that the appropriate analysis was undertaken, enhances defensibility and reduces risks associated with potential spoliation claims. In addition, defensible disposal practices help eliminate future litigation risks associated with information that does not need to be retained.

- *Enhances litigation readiness:* Companies with defensible practices in place enhance their litigation position: They are well-positioned to respond to questions concerning preservation and information management.
- *Enables more focused, rapid litigation response:* Properly managing in a systematic way information that no longer needs to be retained helps to focus litigation defense efforts on known data sources that might potentially be relevant, minimizing unnecessary data clutter and enabling more rapid response efforts.
- *Reduces overall discovery costs by eliminating unnecessary information from the preservation, collection and review sets:* Costs of preserving, collecting and reviewing electronic information are very much in the spotlight these days; implementing good practices upfront helps manage and reduce downstream costs (people, time and money) associated with preserving, collecting and reviewing information that would not otherwise need to be addressed.
- *Saves the company money by reducing IT storage spend:* Storing data costs money; eliminating unneeded data from the overall storage set by implementing defensible practices helps reduce IT costs.
- *Helps the legal department emphasize value-add:* Many in-house legal departments are traditionally viewed by corporate clients as "cost centers." Legal departments can demonstrate value-add to the business by working proactively with business leaders, and with IT, records management, security and other corporate leaders, to implement practices to help reduce operating costs, minimize legal risks, and improve the company's ability to respond rapidly and effectively when litigation arises. Enhancing policies and strategic business practices to consider upfront how information will be managed can dramatically improve the company's risk profile, helping to save time and money, thus leading to better results.

Good information governance practices make good corporate housekeeping sense. Eliminating unnecessary data populations reduces clutter and enhances focus on what is important and relevant. Thoughtful, upfront systematic planning and processes help create the framework for consistency and defensibility. **ACC**

NOTES

[1] "Information Lifecycle Governance Leader Reference Guide: A Model for Improving Information and eDiscovery Economics with Information Lifecycle Governance," *ILG Reference Guide* February 2012V2 (copyright to IBM Corporation, 2010-2012).