

Document and Data Management Considerations for Private Companies

By Kent Clayton and Michael Siersema*

Increasingly, the need for a written, highly structured document and data management policy is becoming vital to any private company. While the recently enacted Sarbanes-Oxley (SOX) rules promulgated by the Securities and Exchange Commission require such a written policy for public companies, there are ample reasons for private companies to also adopt a written document and data management policy.

Various statutes now require most companies, whether public, non-profit or private, to securely maintain written records in regard to certain aspects of their personnel information and business operations. Under the Health Insurance Portability and Accountability Act (HIPAA), for example, companies may be sued if a security breach or other mishap results in the unauthorized disclosure of medical records. The controversial Patriot Act requires disclosure to the federal government of certain customer data and can subject the disclosing company to a lawsuit if the customer was not sufficiently advised of the possibility of such disclosure. A proposed amendment to the federal Rules of Civil Procedure would require lawyers representing parties in litigation to discuss document management systems of their clients prior to any legal proceedings. Another proposed amendment to the federal Rules of Civil Procedure would provide a safe harbor for companies that lose information but have otherwise acted in good faith, precluding any sanctions for such information loss. Certain state laws, such as the California Online Privacy Protection Act of 2003, require website disclosure of privacy policies in regard to personally identifiable information (such as name, address, credit card number, social security number, email address, etc.), which should include a statement about the security procedures in place to protect such information.

Prudence also dictates that written records be maintained in the event of employee claims or litigation involving the company. Companies should also be vigilant in documenting incidents involving any inappropriate or improper behavior by an employee. Emails and instant messages are now often crucial in determining court cases. Employee emails are generally considered to be the property of the employer, and the company's HR policy and employee manual must clearly state so. Accordingly, employers should ensure that copies of all employee emails and instant messages are retained in the event of any employee-related litigation. For the same reason, in addition to maintaining copies of executed contracts and written correspondence, companies should retain copies of all emails and electronic document interchange (EDI) transactions with vendors and customers in the event of any litigation with such third parties. Companies should develop disaster recovery plans and test the recovery of all important data and information. Electronic imaging of physical documents should become standard.

In order to ensure that such procedures are in place and followed, company management must create an infrastructure that will be responsible for the implementation and monitoring of such procedures. This must come from the top down in the organization. The Board of Directors or a committee of the Board should review internal controls and written processes designed to ensure the retention and security of all company records and information and avoid misuse or unauthorized disclosure of such records and information. The Board or such committee should consult closely with members of the company's information technology (IT)

or finance department and others responsible for company files and records in order to ensure compliance with a clearly defined operations policy for the storage, maintenance, protection and destruction of company records and information. There are numerous sources of guidance for company management and IT or finance departments in this regard. These include the Committee of Sponsoring Organizations (COSO), an independent auditing industry group that has received implicit endorsement from the Securities and Exchange Commission. In addition, the Sedona Principles is a set of best practices for e-discovery and the Control Objectives for Information and Related Technology (COBIT) detailing the IT or finance department's role in information and security controls is recommended reading for private companies, even though it is directed at public companies in the post-SOX era.

Company management must also ensure that the IT of finance department has the necessary resources to properly maintain and safeguard electronic records. Extensive storage capabilities and related software are required for document management, data backup, and email and instant message archiving, as such records must be maintained for an extended period of time. Under SOX, for example, records are required to be stored for seven years and must be non-erasable and non-rewritable. Hundreds of outsource storage companies have emerged to assist companies with their e-document management and data storage needs. It is vital that such software and services include fast and reliable document and data search capabilities as well.

Paper records should be organized logically to facilitate their retrieval at a later date. Ideally, the contents of the files should be logged electronically using database software specifically designed for this purpose (the XML standard has gone a long way in standardizing how to identify data). Companies should also ensure that off-site records can be remotely searched.

Access to company records should be closely controlled and restricted to a limited number of individuals. Just as electronic records have audit trails of who has access and when the data was accessed, paper records should not be open and available for anyone to simply walk in and review them, or alter them.

Finally, a document destruction policy should be included as part of the written document and data management policy. Time periods for purges of electronic data and paper records should be established and followed explicitly. As a general rule, it is not recommended that data or records be destroyed until at least seven years has elapsed since the initial archive or storage of such data or records. However, the appropriate time limit depends on many factors, including the nature of the data or records, relevant statutes of limitation and governmental requirements. Company management should therefore consult with legal counsel and a document management professional before establishing a document destruction policy.

* Kent Clayton is a partner and co-chair of the Business Practice Group at Berger Kahn, a full service business law firm with offices in Orange County, Los Angeles, San Diego and the San Francisco Bay area. Michael Siersema is Managing Partner and CEO of Phoenix2000 Group LLC, a technology leadership and advisory services company with offices in Huntington Beach, California, West Lake Village, California and Washington, D.C.