June 2010

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Protecting Confidential Electronically Stored Information

Scenario

A sales person for a large, multi-national corporation keeps confidential customer and sales information on her laptop. During the course of a litigation against the corporation, some of the confidential information must be collected, reviewed and potentially produced. The sales person works at a small, remote office. The in-house lawyer is tasked with ensuring that the confidential information is collected properly, that only appropriate information is produced and that the risk of inadvertent disclosure is minimized.

Types of Confidential Information

Confidential information includes intellectual property, corporate secrets, customer health and financial information, social security numbers, driver's license numbers, customer addresses, credit and debit card information and even Internet browsing habits. Federal and state regulations, such as the Sarbanes-Oxley Act, the Health Information Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, Right to Financial Privacy Act, the Bank Secrecy Act and the Fair and Accurate Credit Transactions Act, have created legal definitions of confidential information, and have established legal requirements for maintaining the privacy of that confidential information. States are also promulgating comprehensive privacy and data breach regulations and disposal requirements to address shortcomings in the existing patchwork federal regulation.

Establishing a Policy for Managing Confidential Information

Corporate policies and procedures should be established to create a uniform approach to the maintenance and potential disclosure of confidential electronically stored information (ESI) in order to properly address the issue of protecting confidential ESI and the obligations that arise as a result of the relevant rules and regulations as well as existing business relationships. These policies and procedures should outline the appropriate steps in the event that there is unauthorized access to ESI containing sensitive personal information. Currently, 47 US states plus the District of Columbia have data breach statutes that require timely notice to affected individuals in the event that their sensitive personal data is subject to unauthorized access. These statutes may also require notification of the state attorney general or other agency, law

enforcement or the consumer reporting agencies. Without policies and procedures setting forth the required steps, it may be difficult to discharge your legal obligations under these laws in a timely manner.

Although technology exists that can help maintain the privacy and security of confidential ESI, its effectiveness depends on the implementation of policies and procedures by organizations to protect the information. Moreover, an established protocol will facilitate the process of responding to a legal request in a timely and sufficient manner, while at the same time protecting privileged and confidential information and minimizing litigation costs.

Identifying Sources of Confidential Information

Companies should be aware of the wide variety of data sources that potentially house their confidential information, including networks, servers, laptops, portable media, shared drives, web sites and backup tapes. It is good practice to maintain an inventory of these sources and the confidential information that is maintained on each. Furthermore, companies should carefully catalog and monitor the confidential information provided to their vendors and take steps to ensure that the vendor maintains adequate policies and procedures to safeguard such information.

Organizations that utilize "cloud computing" need to take additional precautions in addressing confidentiality concerns. The use of integrated internet-based software, including the use of online programs for managing client relationships, maintaining data, and performing other IT-based services creates additional sources that may maintain confidential information, and should be incorporated into all relevant policies and procedures.

Assess Risks Associated with Each Source

After identifying the sources of confidential ESI, organizations should conduct an assessment of the risk associated with the disclosure of the information contained on each source. In conducting that assessment, the organization should consider the relevant regulatory obligations and the likelihood that the source will contain information that will be relevant to litigations. Confidential ESI can then be classified based on the results of the risk assessment, and policies and procedures can be developed for management, storage and backup of the various types of confidential ESI.

Establish Procedures for Maintaining Each Source of Confidential ESI

The policies and procedures for maintaining confidential ESI should establish rules for each data source, with designated custodians for each data type and application. Responsibilities for maintaining the security of these data sources should be allocated among data custodians and the IT department to prevent, identify and repair breaches in security.

It is also important to educate employees regarding the types and forms of confidential ESI that the company maintains, the relevant rules and regulations, the importance of protecting the privacy of that information and the security measures implemented to protect the information. For example, if employees are permitted to maintain confidential information on portable media devices, such as laptops and flash drives, or if employees regularly transmit confidential

information, they should obtain training with respect to the use of data encryption technology or other security devices. To the extent that that sensitive personal information is encrypted, the theft or loss of a portable media device or misdirection of email may not trigger the notice requirements under the state data breach laws.

A protocol should be incorporated for the regular updating of confidentiality policies and procedures. This may require the organization to periodically assess new sources of confidential information, new mechanisms to protect that information and new rules and regulations. In addition, organizations should consider periodically auditing the existing security measures.

Protecting Confidential ESI Requested During Discovery

A litigation or government investigation may require the production of confidential and private information. In civil litigation, it is common for the parties to enter into confidentiality agreements that dictate how confidential information will be treated. Pursuant to Rule 26(c) of the Federal Rules of Civil Procedure, a party may seek a protective order providing that confidential information may not be revealed or that it must be used in a limited manner. Protective orders and confidentiality agreement are sometimes reviewed and approved by the courts. Relevant factors to consider in drafting a protective order or a confidentiality agreement include:

- A tiered approached to confidentiality designations (for example, designations of confidential and highly confidential)
- Case-specific definitions of what would fall into each tier of confidentiality
- The manner in which confidential information can be used (for example, attorney's eyes only)
- Procedures for use of confidential information in court filings, at depositions, at trial and in expert discovery
- Use of confidential information outside of the litigation or investigation
- Production of confidential information in response to requests from third parties
- Return or destruction of confidential information after a litigation has concluded
- Procedures to correct an inadvertent failure to designate a document containing confidential information
- Procedures to challenge a confidentiality designation

Keeping confidential ESI protected should not be the concern of only the Risk Management and IT departments. Knowing where confidential ESI is kept, and having policies and procedures to maintain the confidentiality, will enhance protective measures needed due to inadvertent loss or required production.

For inquiries related to this Tip of the Month, please contact Jeffrey P. Taft at jtaft@mayerbrown.com, Kim Leffert at kleffert@mayerbrown.com or Rebecca Kahan at rkahan@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact

Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com or Thomas A. Lidbury at tlidbury@mayerbrown.com.

Learn more about Mayer Brown's Privacy & Security practice or contact Rebecca S. Eisner at reisner@mayerbrown.com, John P. Mancini at jmancini@mayerbrown.com or Jeffrey P. Taft at jtaft@mayerbrown.com.

Please visit us at www.mayerbrown.com