

This article originally appeared in the December 1999 edition of *The Health Lawyer*, a publication by the ABA Health Law Section

Proposed Federal Privacy Rules: Locking the Electronic File Cabinet

By Stephen L. Page and Deborah W. Larios

Introduction

On November 3, 1999, the U.S. Department of Health and Human Services ("HHS") issued a proposed rule (the "Rule") that would establish standards to protect the privacy of health information. The Rule covers individually identifiable health information that is or has been electronically maintained or transmitted by health care providers, health plans, and health care clearing-houses, even if the information is no longer in electronic form. HHS was required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to propose the Rule because Congress failed to enact privacy legislation by the statutory deadline of August 21, 1999. Comments on the Rule will be accepted until January 3, 2000. HHS is required by HIPAA to promulgate the final rule no later than February 21, 2000.

Under the Rule, patients may access, amend and correct, and receive an accounting of the disclosure of their health information. Health care organizations may not use or disclose health information unless permitted under the Rule or pursuant to an individual's authorization. Finally, health care organizations must implement administrative processes to respond to patient complaints and to protect health information.

Federal officials estimate that compliance with the Rule will cost the health care industry \$3.8 billion over 5 years, but the insurance industry estimates that the cost could be 10 times that amount. According to federal officials, the cost to health care providers and plans to issue notices informing patients of their privacy rights will be more than \$400 million. In addition, as thousands of patients try to correct their health information, federal officials estimate that the cost to the health care industry to respond to these requests will be more than \$2 billion over the next 5 years.

The operational impact to health care organizations is likely to be far-reaching because of the difficulty in determining and keeping track of what information is covered. The Rule protects the health care information itself, not just a particular record. Once the information has been electronically transmitted or stored, it is protected by the Rule even if reprinted, discussed orally, viewed from a computer screen, or included in paper files that were compiled long before the electronic transmission took place. The situation becomes further complicated if the protected information is mixed with unprotected information about an individual. To assure compliance, health care organizations may have to treat *all* individually identifiable health information in their possession in accordance with the Rule.

Once the final rule is promulgated, health care organizations will have two years to achieve total compliance with the final rule. Due to the complexities of the Rule's requirements, health care organizations should begin reviewing their current health information privacy policies and procedures in order to get a head start on what will almost certainly be a time-consuming and expensive process.

Who Must Comply With the Rule?

The Rule covers almost every organization or individual that comes into contact with patient information, from the initial patient encounter to the payment for the medical care or supplies. Specifically, the Rule applies to health plans, health care clearinghouses, and health care providers who electronically maintain or transmit individually identifiable health information.

Health Care Providers. Under the Rule, a health care provider is a provider of services as defined in Section 1861(u) of the Social Security Act, a provider of medical or other health services as defined in Section 1861(s) of the Social Security Act, and any other person who furnishes, bills, or is paid for health care services or supplies in the normal course of business ("Providers"). Examples of Providers include physicians, hospitals, skilled nursing facilities, home health agencies, licensed or certified health care practitioners, and pharmacies.



Health Plans. The Rule covers almost all third-party payors and government payors of health care. Under the Rule, a health plan is an individual or group plan that provides or pays the cost of medical care, including agencies administering government funded or assisted programs (“Plans”). The Rule lists sixteen types of Plans. Examples of Plans include health maintenance organizations, employee welfare benefit plans, Medicare Part A and B, and Medicaid.

Clearinghouses. The Rule covers organizations, known as clearinghouses, that transfer and/or convert health information into standard data elements between Providers and Plans. HIPAA requires that Providers and Plans be able to exchange health information relating to certain financial and administrative activities (such as health claims, payments, and remittance advices) using standard data elements. Under the Rule, a health care clearinghouse is a public or private entity that processes or facilitates the processing of nonstandard data elements of this health information into standard data elements (“Clearinghouses”). For example, a Clearinghouse would receive information from a hospital and translate the data from a proprietary format into a standard format and forward data to a health maintenance organization or its Clearinghouse. Examples of Clearing-houses include billing services, repricing companies, third-party administrators, and “value-added” networks. Because Clearinghouses seldom deal directly with individuals, the Rule exempts them from a number of requirements unless they are acting on behalf of a Plan or Provider.

What Health Information is Protected by the Rule?

The Rule applies to “individually identifiable health information” that is or has been “electronically transmitted or maintained” by a Provider, Plan, or Clearinghouse (“Protected Health Information”). Once the individually identifiable health information is electronically transmitted or maintained, it remains protected in any other form in the possession of the Provider, Plan, or Clearinghouse. For example, the information remains protected after it is read from a computer screen and discussed orally, printed onto paper or other media, photographed, or otherwise duplicated.

Individually identifiable health information. Individually identifiable health information is limited to information that contains the following elements. First, the information must relate to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. Second, the information must be created by or received by a Provider, Plan, Clearinghouse, or employer. Third, the information must identify or there must be a reasonable basis to believe that the information can be used to identify an individual. Identifying information includes demographic information collected from the individual.

Information that is electronically transmitted and maintained. Information is “electronically transmitted” when it is exchanged with a computer using electronic media. The key is whether the source or target of the exchange is a computer. Examples include the physical movement of information from one location to another by floppy disk and transmissions over the Internet, Extranet, leased lines, dial-up lines, and private networks. Telephone voice response and “faxback” (*i.e.*, a request for information from a computer made via voice or telephone keypad input with the requested information returned as a fax) systems would be included because these are computer output devices similar in function to a printer or video screen. “Electronically transmitted” does not include “paper-to-paper” faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail. Information is “electronically maintained” if it is stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc (CD) optical media.

What Does the Rule Require?

The Rule contains requirements relating to: (i) the disclosure and use of Protected Health Information; (ii) an individual’s rights with respect to his Protected Health Information; (iii) administrative systems that must be implemented by Providers, Plans, and Clearinghouses; and (iv) contractual provisions that Providers, Plans, and Clearinghouses must enter into with their agents.



The Disclosure and Use of Protected Health Information. A Provider, Plan, and Clearinghouse may only disclose or use Protected Health Information when required or permitted by the Rule. A Provider, Plan, or Clearinghouse is *required* to disclose Protected Health Information when an individual requests access to his Protected Health Information, as discussed below, and when the Secretary of HHS requests access when investigating compliance with the Rule. A Provider, Plan, or Clearinghouse is *permitted* to use or disclose Protected Health Information for the following purposes -- to treat a patient, to obtain payment, to carry out its internal operations, and for certain public uses. The Provider, Plan, or Clearinghouse is not required to obtain written authorization from the individual for these uses or disclosures, and in fact is *prohibited* from seeking such authorization unless required by state law. Any authorization required by state law must be separate from an authorization required by the Rule. A Provider or Plan and an individual also may mutually agree that any Protected Health Information used and disclosed for treatment, payment, or health care operations be further restricted, subject to certain limitations. The Provider, Plan, or Clearinghouse is also permitted to disclose Protected Health Information with appropriate written authorization.

Treatment. The Provider, Plan, or Clearinghouse may use and disclose Protected Health Information to treat a patient. Treating the patient includes not only the provision of health care, but also the coordination of health care among health care providers (including health care management of the individual through risk assessment, case management, and disease management) and referral of a patient from one provider to another provider.

Payment. The Provider, Plan, or Clearinghouse may use or disclose Protected Health Information to obtain payment. Under the Rule, payment means activities undertaken by or on behalf of a Plan or Provider to obtain premiums or to determine or fulfill its responsibility for coverage under the health plan and for provision of benefits under the health plan, or to obtain reimbursement for the provision of health care. The Rule authorizes five payment-related activities.

Health Care Operations. The Provider, Plan, or Clearinghouse may use or disclose Protected Health Information to perform its operations. Health care operations means the activities listed below when undertaken by or on behalf of the Provider or Plan for the purpose of carrying out the management functions of such entity necessary for the support of treatment or payment, quality assurance, utilization review, audits, credentialing, and similar activities. The Rule lists five activities that are considered health care operations.

Public Uses. The Provider, Plan, or Clearinghouse may use or disclose Protected Health Information for the following public uses: (i) verification that it has implemented certain administrative standards required by the Rule; (ii) public health activities (such as reporting a disease, injury, or vital event such as birth or death; public health surveillance; or reports of child abuse or neglect); (iii) health oversight activities, including audit, investigation, inspection, and civil, criminal, or administrative proceedings; (iv) use in the course of any judicial and administrative proceedings; (v) disclosures to coroners, including medical examiners; (vi) disclosures for law enforcement purposes; (vii) intelligence and national security activities; (viii) health care fraud; (ix) urgent circumstances; (x) disclosure and use for governmental health data systems; (xi) facility patient directory information; (xii) banking and payment purposes; and (xiii) research purposes. The Rule contains specific requirements and limitations for each of the above items that must be met prior to disclosure or use by the Provider, Plan, or Clearinghouse.

Patient Authorization. The Provider, Plan, or Clearinghouse may use or disclose Protected Health Information pursuant to an individual's authorization that complies with the Rule. If the individual initiates the disclosure, the authorization must include several specific items, including but not limited to an expiration date and a statement that the individual may revoke the authorization at any time. For example, an individual may seek disclosure when an individual applies for life or disability insurance or seeks certain job assignments where health is relevant, or when an individual's attorney needs the information in tort litigation. If the Provider, Plan, or Clearinghouse initiates the request for disclosure or use, the authorization must include all of the items required for an individually initiated disclosure and must also inform the individual of the purpose of the disclosure and whether the disclosure will result in payment to the Provider, Plan, or Clearinghouse. The



Provider, Plan, or Clearinghouse must obtain an individual's authorization if it wishes to disclose or use Protected Health Information for any of the following purposes: (i) marketing of health and non-health items and services; (ii) disclosures for sale, rental, or barter; (iii) use and disclosure to non-health related divisions of the organization, for example for use and marketing of life and casualty insurance or banking services; (iv) disclosure to a Plan or Provider for making eligibility or enrollment determinations or for underwriting or risk-rating determinations; (v) disclosure to an employer for use of employment determinations; and (vi) use or disclosure for fund-raising purposes.

The Rule includes a model authorization form. The model is a unitary model, which includes all of the requirements for authorizations initiated either by the individual or by the Plan or Provider. If the model authorization form is not used, the authorization form must be written in plain language.

When the use or disclosure of the Protected Health Information is permitted under the Rule, a Provider, Plan, or Clearinghouse must make all reasonable efforts to use or disclose no more than the minimum amount of information necessary to accomplish the relevant purpose, taking into consideration practical and technological limitations. The Rule also prohibits a Provider, Plan, or Clearinghouse from disclosing psychotherapy notes, as defined by the Rule, for treatment, payment, or health care operations unless specifically authorized by the individual.

Exception for De-identified Information. To encourage Providers, Plans, and Clearinghouses to delete identifying information from Protected Health Information, the Rule permits a Provider, Plan, or Clearinghouse to use and disclose de-identified information, provided that:

1. it does not disclose the key or other mechanism that would enable the information to be re-identified, and
2. it has no reason to believe that such use or disclosure will result in the use or disclosure of protected health information (e.g., because the recipient has the means to re-identify the information).

Protected Health Information is presumed not to be "identifiable" if:

1. all of the following data elements have been removed or otherwise concealed: name; address, including street address, city, county, zip code, or equivalent geocodes; names of relatives and employers; birth date; telephone and fax numbers; e-mail addresses; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; any vehicle or other device serial number; web URL; Internet Protocol (IP) address; finger or voice prints; photo-graphic images; and any other unique identifying number, characteristic, or code (whether generally available in the public realm or not) that the organization has reason to believe may be available to an anticipated recipient of the information, and
2. the organization has no reason to believe that any reasonably anticipated recipient of such information could use the information alone, or in combination with other information, to identify an individual.

An Individual's Rights with Respect to His Protected Health Information. The Rule grants several basic rights to an individual with respect to his Protected Health Information. These include the right of an individual to: (i) review and copy his Protected Health Information; (ii) amend and correct his Protected Health information; (iii) receive an accounting of how his Protected Health Information has been used or disclosed; and (iv) receive written notice of how his Protected Health Information will be used or disclosed by the Provider and Plan.



Access. An individual has the right to inspect and copy his Protected Health Information. An individual's request to inspect or copy the information may be denied in certain circumstances, including when the information was compiled in reasonable anticipation of a legal proceeding or when a licensed health care professional has reasonably determined that the disclosure of the information would likely endanger the life or physical safety of the individual or another person. The Rule contains requirements that must be implemented to process such requests and denials of such requests. Action must be taken on an individual's request to review the Protected Health Information as soon as possible, but no later than within 30 days after the request.

Corrections. An individual has the right to request an amendment or correction of any inaccurate or incomplete Protected Health Information. The individual's request may be denied when the information: (i) was not created by the Provider or Plan; (ii) is not available for access or copying because of a permitted denial of a patient's right of access; or (iii) is accurate and complete. The Rule contains requirements that must be implemented to determine whether requests should be granted or denied. The Rule also addresses how to process the amendment or correction (including notifying parties that may have received the inaccurate or incomplete information) and how to process denials (including a statement by the patient and a rebuttal). Action must be taken on an individual's request to amend or correct within 60 days of the request.

Accounting of Use and Disclosure. An individual can request an accounting of all disclosures of his Protected Health Information by a Provider, Plan, or Clearinghouse for purposes other than treatment, payment, health care operations, and, under certain circumstances, disclosure to health oversight agencies or law enforcement agencies. The accounting must include all of the following: (i) the date of the disclosure; (ii) the name and address of each organization which received the information; (iii) a brief description of the information disclosed; (iv) the purpose for which the information was disclosed (for disclosures not requested by the individual); and (v) a copy of all requests and authorizations for disclosure. The accounting must be provided to the individual as soon as possible, but no later than 30 days from receipt of the request.

Notice of Use and Disclosure. An individual has the right to receive a written notice from Providers or Plans regarding their Protected Health Information policies. The notice must describe the uses and disclosures that will be made without individual authorization, and distinguish between those uses and disclosures that are required by law and those that are permitted but not required by law.

Specifically, the notice must state that:

1. Other uses and disclosures will be made only with the individual's authorization and that such authorization may be revoked.
2. An individual may request that certain uses and disclosures of his or her protected health information be restricted, and the organization is not required to agree to such a request.
3. An individual has the right to request, and a description of the procedures for exercising, the following with respect to his Protected Health Information:
 - (a) Inspection and copying;
 - (b) Amendment or correction; and
 - (c) An accounting of the disclosures of such information by the covered entity.
4. The organization is required by law to protect the privacy of its individually identifiable health information, provide a notice of its policies and procedures with respect to such information, and abide by the terms of the notice currently in effect.



5. The organization may change its policies and procedures relating to protected health information at any time, with a description of how individuals will be informed of material changes.
6. Individuals may complain to the covered entity and to the Secretary of HHS if they believe their privacy rights have been violated.
7. The name and telephone number of a contact person and the date the version of the notice was produced.

An example of a privacy notice is included in the Rule. Plans must distribute notices to their enrollees no later than the effective date of the Rule and to each new enrollee at the time of enrollment. Providers must give notices to patients at the time of first service delivery and must post the notice in their offices.

What Administrative Systems are Required?

Providers, Plans, and Clearing-houses must adopt administrative systems, including written policies and procedures, that enable them to address patient concerns and protect health information in accordance with the Rule. Specifically, Providers, Plans, and Clearinghouses must implement the measures outlined below.

1. Designate a privacy official who is responsible for the development and implementation of privacy policies and procedures.
2. Provide privacy training to members of its workforce and require its workforce to certify completion of the training and compliance with the organization's policies and procedures required by the Rule at least once every three years.
3. Implement appropriate administrative, technical, and physical safeguards to protect the privacy of Protected Health Information, including reasonable standards to verify the identity and authority of persons requesting information. On August 12, 1998, the Secretary of HHS proposed a rule setting forth standards for the security of individual health information for use by Providers, Plans, and Clearinghouses.
4. Develop a system of appropriate sanctions for members of its workforce, vendors, and agents, discussed below, who violate the organization's policies.
5. Implement safeguards to ensure Protected Health Information is not used inappropriately by its workforce, vendors, and agents.
6. Provide a means for individuals to lodge complaints about the organization's information practices and maintain a record of any complaints.
7. Have procedures for mitigating to the extent practicable any deleterious effect of an inappropriate disclosure or use of Protected Health Information.
8. Provide a written notice of the organization's information practices, as discussed above.
9. Designate a contact person (who may also be the privacy official) who is responsible for answering questions regarding the organization's information practices and for receiving complaints concerning the organization's noncompliance with the Rule.

The detailed policies and procedures that an organization must adopt for meeting these standards are left to the discretion of each Plan, Provider, or Clearinghouse. Each entity must assess its own needs and implement privacy policies appropriate to its information practices and business requirements.



How Does the Rule Apply to the Agents of Providers, Plans, and Clearinghouses?

Most Providers and Plans outsource a significant number of functions to third parties that expose the third party to Protected Health Information. Examples include accrediting organizations, attorneys, auditors, consultants, health care clearinghouses, value-added networks and switches, third-party administrators, physician practice management companies, data processing firms, and billing firms.

A Provider, Plan, or Clearinghouse may not disclose Protected Health Information to a third party who assists or performs a function or activity on behalf of the Provider, Plan, or Clearinghouse, unless the third party enters into a contract that contains several provisions required by the Rule. Under the Rule, these third parties are called business partners ("Business Partners"). Business Partners do not include an employee or a volunteer associated with the Provider, Plan, or Clearinghouse on a paid or unpaid basis. Business Partners also do not include third parties where the third party is providing treatment, consultation, or a referral.

The contract between the Business Partner and the Provider, Plan, or Clearinghouse must include the following provisions:

Restriction of Use and Further Disclosure and Compliance with the Rule. The Business Partner may not use or further disclose the information other than as permitted by the contract. The Business Partner may not use or further disclose the information in a manner that would violate the requirements of the Rule if done by the Provider, Plan, or Clearinghouse.

Implement Safeguards to Protect the Health Information. The Business Partner must implement appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract.

Report Inappropriate Use or Disclosure. The Business Partner must report to the Provider, Plan, or Clearinghouse any use or disclosure of the information not provided for by its contract of which it becomes aware.

Police its Subcontractors. The Business Partner must ensure that any subcontractors or agents to whom it provides Protected Health Information received from the Provider, Plan, or Clearinghouse agree to the same restrictions and conditions that apply to the Business Partner with respect to such information.

Compliance with an Individual's Rights with Respect to the Protected Health Information. The Business Partner must make Protected Health Information available in accordance with the individual's rights outlined above and incorporate any corrections or amendments approved by the Provider, Plan, or Clearinghouse as outlined above.

Access by Secretary of HHS. The Business Partner must make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary of HHS for determining the compliance with the Rule by the Provider, Plan, or Clearinghouse.

Termination Provisions. The Business Partner must return or destroy all Protected Health Information upon termination of the contract. The Provider, Plan, or Clearinghouse must be able to terminate the contract if it determines that the Business Partner has violated a material term of the contract.

Third-party Beneficiary. The contract must state that individuals whose Protected Health Information is disclosed pursuant to the contract are intended third-party beneficiaries of the contract.

A material breach by a Business Partner of its obligations under the contract will be considered noncompliance by the Provider, Plan, or Clearinghouse if the Provider, Plan, or Clearinghouse knew or reasonably should have known of such breach and failed to take reasonable steps to terminate the contract or to ensure the Business Partner cured the breach.



Does the Rule Preempt State Laws?

The Rule preempts a state law that is contrary to the Rule. State laws not only include statutes and regulations, but also court decisions and other actions having the effect of law. A state law is contrary to the Rule when a party: (i) would find it impossible to comply with both the state law and the Rule, or (ii) the state law is an obstacle to the execution of the objectives of Part C of Title IV of the Social Security Act or Section 264 of HIPAA.

Due to the numerous exceptions to preemption by the Rule, the Rule does not establish uniform privacy standards. As a practical matter, the Rule serves as a floor below which state privacy laws may not go. For example, state laws that relate to the privacy of health information that are more stringent and restrictive are not preempted by the Rule. States have numerous privacy laws which must be reviewed for preemption. In 1999 alone, state lawmakers in 35 states have introduced more than 300 bills relating to the confidentiality of medical records.

Further, the Rule does not preempt a state law if the Secretary of HHS determines that the state law: (i) addresses controlled substances; (ii) is necessary to prevent fraud and abuse; (iii) ensures appropriate state regulation of insurance and health plans; (iv) enables state reporting on health care delivery or costs; or (v) improves the Medicare or Medicaid Program or efficiency and effectiveness of the health care system. The Rule includes lengthy provisions for determining whether a state law is not subject to preemption due to an exemption, including an advisory opinion process. Preemption is a major issue under the Rule and is likely to be the topic of considerable debate in the future.

What Are the Penalties?

The Secretary may impose civil monetary penalties against Providers, Plans, and Clearinghouses who fail to comply with the requirements of the Rule. Civil monetary penalties are capped annually at \$25,000 for each standard that is violated. Although the Rule does not contain a private cause of action for individuals whose Protected Health Information has been improperly disclosed or used, the Rule may indirectly provide a contractual private cause of action because it requires Providers and Plans and their Business Partners to state in their agreements that individuals whose Protected Health Information is disclosed pursuant to the agreement are intended third-party beneficiaries. The Rule also requires the HHS to conduct compliance reviews, and allows individuals to file complaints with the Secretary of HHS if a Provider, Plan, or Clearinghouse fails to comply with the Rule.

HIPAA provides that a Provider, Plan, or Clearinghouse may assert several defenses in the event the Secretary of HHS assesses a penalty. However, a penalty may not be imposed if the Provider, Plan, or Clearinghouse establishes to the satisfaction of the Secretary of HHS that it did not know, and by exercising reasonable diligence would not have known, that it had violated the standard. Additionally, a penalty may not be imposed if the Provider, Plan, or Clearinghouse corrects a failure to comply within 30 days of determining a violation occurred and the failure to comply was due to reasonable cause rather than willful neglect. Finally, the Secretary of HHS may waive or reduce the penalty if it would be excessive relative to the compliance failure, and the compliance failure was due to reasonable cause and not willful neglect.

HIPAA also establishes criminal penalties for wrongful disclosures of "individually identifiable health information." A person who knowingly discloses individually identifiable health information improperly to another person can be fined not more than \$50,000, imprisoned not more than one year, or both. If the offense is committed under false pretenses, a person can be fined not more than \$100,000, imprisoned for not more than five years, or both. If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a person can be fined not more than \$250,000, imprisoned not more than ten years, or both.



Conclusion

A comprehensive federal privacy law is long overdue. The current health care system allows individuals far removed from the patient's physician or other provider to have access and use a patient's most private information, while providing the patient with little or no recourse against such individuals for improper use or disclosure. Current technology allows providers, employers, and plans to compile and cross-reference an individual's health information for virtually any purpose. Further, the complexity of the current health care system requires most health information to cross state lines. In order to address these driving forces, federal privacy law should provide uniformity and clarity regarding when and how a patient's health information can be used and disclosed.

In its present form, the Rule falls short of meeting these goals. The Rule does not provide uniformity since Providers and Plans may still have to comply with many varied state laws that are not preempted by the Rule. The Rule also provides little clarity due to the confusion that will arise when health care organizations try to determine, for example, whether the use and disclosure of the health information is subject to an exemption; whether the Provider and Plan have received an acceptable authorization from the proper individual who is competent to make such an authorization; and whether the Provider and Plan have used or disclosed only the minimal necessary information for a permitted purpose.

Instead of leaving HHS to promulgate a complex rule that satisfies no one, many patients, providers, and plans may want to renew their efforts to encourage Congress to enact an effective and simple law such as one that preempts all state laws and allows a private cause of action when a patient has been clearly and severely damaged as a result of an improper use or disclosure of his health information.

Stephen L. Page is an associate in the Health Law Group and E-Commerce and Internet Law Group at Waller Lansden Dortch and Davis, PLLC. Mr. Page's practice focuses on advising clients in the health care industry on regulatory and transactional matters. Prior to joining Waller Lansden, Mr. Page worked with financial services clients in the telecommunications industry to implement financial electronic data interchange systems. Mr. Page graduated cum laude from the University of Tennessee College of Law.

Deborah W. Larios is a member of the law firm of Waller Lansden Dortch & Davis, PLLC. She graduated magna cum laude and Phi Beta Kappa from Vanderbilt University and also received her J.D. from Vanderbilt. Ms. Larios works with health care providers on such issues as fraud and abuse, the Stark law, compliance, informed consent, medical records, confidentiality issues, reimbursement, and related health care operations. She is a member of the American Health Lawyers Association, the American Bar Association (Antitrust and Health Law Sections), the Tennessee Bar Association (current chair, health law section), and the Nashville Bar Association (out-going chair, health law section).