INSIDE THE MINDS

Complying with Health Care Privacy Laws

Leading Lawyers on Maintaining Privacy and Security Compliance, Managing Liability, and Understanding Recent Developments

ASPATORE

First Printing, 2008
10 9 8 7 6 5 4 3 2 1

Effective Implementation of Privacy Compliance Programs

Linda A. Malek

Partner

Moses & Singer LLP

ASPATORE

Introduction

Our law firm is a full service practice, although there are certain areas in which we typically specialize. One of those areas is privacy; I chair our firm's Privacy Practice Group as well as its Health Care Practice Group. We deal with privacy issues for a variety of sectors of the health care industry, ranging from pharmaceuticals to academic medical centers and their clinical research activities, as well as health plans and institutional providers. We also work on a variety of clinical research issues aside from privacy, for both pharmaceutical companies and academic medical centers. We represent a number of managed care entities and work on a whole host of issues for those clients, from provider contracting issues, to regulatory counseling, to mergers and acquisitions. We also do a lot of work in the context of regulation, generally with respect to Medicare and Medicaid compliance issues, fraud, and abuse.

Our practice is unique in the respect that because we are a midsize firm, every attorney in the practice has to keep current on a broad range of industry laws and regulations, which are constantly changing, and every attorney who is working on a matter will be working on it from start to finish. Large firms are often highly segmented—they have regulatory lawyers who only look at regulatory issues, and transactional lawyers who only deal with transactions; we take a different approach. However, I prefer the approach we take, because I think it allows us to have a better and more comprehensive understanding of the various issues facing our clients in a given project or transaction.

Privacy and Security Law Concerns for Health Care Clients

What is currently taking place in the privacy law context extends well beyond the Health Insurance Portability and Accountability Act (HIPAA); issues are now arising in the context of state security breach notification laws, and other state laws as well. In addition, there are other federal laws governing privacy that are not specific to health care but end up having an impact on the health care arena, such as the CAN-SPAM Act. A great deal of activity in terms of legislation has affected the pharmaceutical industry in particular because of its marketing activities and clients in that industry need to be aware of these trends.

Pharmaceutical companies are not considered covered entities under HIPAA; therefore, many of these companies may not have initially contemplated that privacy would become such a significant concern. However, many other privacy laws such as those in Texas and California, for example, have since been promulgated that do affect these companies directly, and to the extent that pharmaceutical firms are partnering with entities that are covered by HIPAA—e.g. in the context of research—they have an interest in making sure that those entities comply with HIPAA in order for the research activities to be unimpeded by concerns about non-compliance.

Indeed, when pharmaceutical companies sponsor research they have an interest in ensuring that they can use the results and that the integrity of the research is maintained. Additionally, when engaging in marketing activities, compliance with applicable privacy laws is important as well. Therefore, we are seeing a growing number of clients that are engaging in a best practices approach with respect to privacy that is useful to them both from a reputational and a practical standpoint. Because pharmaceutical companies typically operate in a number of states and countries they must take an approach to privacy issues that is somewhat different from entities covered by HIPAA, in that they need to make sure that they are complying with the most stringent state laws. Therefore, I believe that the challenges pharmaceutical companies face in this area are in some ways greater than those facing other companies, because what rules apply to them and how they comply with those rules is sometimes less clear.

We are currently seeing a lot of legislative activity on the federal level with respect to privacy and security issues, including efforts to harmonize the various state laws—for example, in the context of security breach notification—in order to create a federal standard, and with respect to certain marketing laws that are state specific. This is a continually developing area that will be important to monitor on an ongoing basis.

Privacy and Security Compliance Challenges for the Health Care Sector

A significant compliance challenge for entities that are subject to HIPAA is to be continually aware of legislative and regulatory developments with

respect to privacy laws in the states in which they are operating, as well as such developments on the federal level that could dovetail with their compliance obligations under HIPAA. For example, I recently worked on a U.S. Department of Health and Human Services project that involved looking at the intersection of HIPAA and the FTC Act's deceptive acts and practices provisions, and enforcement in that area. We found that there is quite a bit of intersection between those laws in terms of the FTC's authority to enforce, for example, a notice of privacy practices posted on Web sites of organizations covered by HIPAA (covered entities), but many health care entities may not think about these issues in those terms because they are unaware of how these laws that are not specifically targeted toward the health care industry may be applicable to them. Consequently, most health care organizations tend to have a very well-established infrastructure to comply with HIPAA, with training programs, and comprehensive policies and procedures, but they may not take a comprehensive approach to privacy compliance generally, by looking at how different laws may apply to their activities.

Therefore, the challenge for health care companies is to have a privacy and security compliance program that is vigilant about staying up to date with all of the other laws that could be applicable to their business and operations. Privacy and security are areas that are continually developing on both the federal and state levels.

Health Care Privacy Laws

Key Compliance Issues for Health Care Clients

Health care privacy and security issues are inextricably linked—you cannot have one without the other. In order to protect privacy you must have adequate security, and security takes many different forms. Security is not limited to protecting electronic information; it also extends to physical measures such as keeping files locked, and creating a corporate culture of maintaining confidentiality. Indeed, many massive security breaches have been caused by an employee losing a handheld device or having a laptop stolen from his or her car. These breaches could possibly have been prevented or mitigated if the organization had policies in place with respect to removing such information from the office setting, or if it had installed

adequate control mechanisms on a remote device so that if it were to be stolen the information could be wiped clean from another location.

The Centers for Medicare and Medicaid Services (CMS) recently promulgated a sample interview and document request form to be used for HIPAA security onsite investigations and compliance reviews. Many of our clients were previously unaware of this document, but it is a very helpful resource to assist entities in their own internal review of their security infrastructure. It would behoove health care entities to examine this checklist and ensure that all necessary security measures are in place in anticipation of any CMS audit and as a matter of best practices generally.

Many entities that are covered by HIPAA put solid compliance measures in place when the Privacy and Security Rules were enacted but have not revisited such measures in depth since then because it has been many years since HIPAA was enacted. Consequently, we often find that certain habits have formed with respect to privacy and security law compliance that are not necessarily good habits and therefore compliance practices need to be regularly examined and updated. A privacy officer should perform internal compliance audits from time to time in order to get a sense of the culture of the organization and what compliance practices are being adhered to. When a new person comes into that capacity, we will often be called in to help him/her gauge the current compliance culture. We will talk to various personnel so that we can obtain a sense of where the client organization currently is in terms of privacy and security law compliance. We will then counsel the client based on what we see is indicated in terms of remediation.

Best Practices for Privacy Compliance Programs

A health care entity that operates in multiple jurisdictions must be sure that it is complying with the most stringent laws that apply to the jurisdictions in which it operates. For example, if a health care entity operates in three states and it is covered by HIPAA, it is also covered by state laws that vary in their stringency. Taking a best practices approach as opposed to having bifurcated compliance programs is the best way to ensure that all departments throughout the company that handle confidential information are complying with the same standard. In some instances, a health care

company may even be doing more than it needs to do, but at minimum, it will be acting in compliance with all applicable laws.

Another important best practice is to fully educate the health care organization's staff and line personnel so that they have a solid understanding of what their compliance obligations are and what compliance means from a practical context. For example, if personnel are not adequately trained to apply the organization's policies and procedures to their day-to-day activities, and are not given frequent reinforcement training, then an organization runs the risk that individuals in the workplace will not understand how changes in the law will affect their duties. Therefore, it is important to have training sessions on a regular basis. It is also important to communicate within each department, as well as to practice an enterprise-wide approach to compliance across departments so that personnel have a strong grasp of how confidential information is accessed and shared throughout the organization.

Health care companies must be very proactive if a security breach is determined. We will often receive calls from clients who have found that there has been an internal security breach and want to know what their obligations are. In such cases, we typically advise the client that even if they have very little in the way of legal obligations to the consumer whose information has been breached, the organization should think about the breach in terms of its own reputational risks. Such risks should always be part of the calculation when considering what measures should be taken to mitigate a breach, and they should also be part of the calculation in terms of how an entity approaches compliance as a whole, because in order to be considered a trusted holder of confidential information you must be able to show that privacy compliance is taken very seriously and that you conform to the highest industry standards regarding the protection of such information.

Evaluating and Updating a Compliance Program

Our ability to evaluate and update a compliance program on behalf of a health care client largely depends on how much the client allows us to do in terms of examining the policies they have in place and talking to their personnel. In some instances, we are asked to perform an overall analysis,

and in other instances we are called in about very specific issues such as how to best mitigate a breach of privacy or security if one occurs.

We always let our clients know about new legislation or regulations that are either in the process of being promulgated or which have already been promulgated if they are likely to affect their business. We will then usually follow up to find out if the client has taken steps to implement new measures to comply with these laws. When we inform clients of a change in the law, we may then be asked to come in and review their policies and update them or review certain contracts for amendment, but other times the infrastructure within the entity will be sufficient so that they can do the job themselves. In either case, we are always on the lookout to keep our clients updated so that they are aware of changes in the laws as they happen.

It is very important that health care organizations talk to their counterparts within their industry sector so that they are aware of current best practices in their industry. At the same time, health care clients should communicate with their outside counsel on a regular basis so that they are aware of new industry best practices, and how they can approach implementing them within their own organization. Finally, performing periodic internal audits is essential, because the only way for an organization to become aware of what needs to be changed or updated in terms of its compliance practices is to conduct an audit that allows key decision makers to know what practices are actually occurring within the company.

Organization-Specific Compliance Practices

Those privacy and security compliance practices that should be considered the most important and/or essential will vary, depending on the specific health care organization. For example, an academic medical center may be engaging in patient care and clinical research, and the issues that arise in those contexts will intersect with informed consent issues in such areas as the use and disclosure of genomic information, as well as in the context of posting research information electronically in order to comply with clinical trial transparency requirements. Therefore, we counsel such clients on compliance practices that are specific to the use and disclosure of research subject information in the context of the clinical research activities in which they are involved.

Also in the context of clinical research, when coming up with compliance practices with respect to the use and disclosure of private research subject information, we try to harmonize the requirements of various privacy laws with the other applicable requirements under National Institutes of Health (NIH) guidelines, Office of Human Research Protections (OHRP), and Food and Drug Administration (FDA) requirements. Sometimes there are inconsistencies among those requirements, and we then contact the relevant agencies to inform them of the inconsistency and try to obtain guidance. In some instances, the agencies will then communicate with one another on the issue and then provide formal or informal guidance. Indeed, in the academic research area there are so many different laws at issue to protect the patient that they sometimes appear to be inconsistent with each other, and we need to counsel the client in terms of harmonizing those provisions.

Developing a privacy compliance program in the pharmaceutical industry context poses different challenges, because such companies need to use specific consumer information for various purposes, such as for marketing initiatives. In those cases, we counsel the client on applying a whole host of federal and state laws that may or may not be specific to health care but are specific to privacy and consumer protection issues. It is important for pharmaceutical companies to take a best practices approach to compliance, both for reputational purposes but also for practical purposes, because many pharmaceutical companies operate all over the country and all over the world. We try to find a way for these clients to do what they need to do when it comes to marketing, but they must also establish at least a base line standard of privacy compliance practices so that they can carry out their initiatives while still remaining in compliance with all applicable privacy and security laws.

For health plan clients, privacy and security issues arise in a variety of contexts, depending on the specific activities in which the health plan is involved. Health plans typically have an abundance of claims data that could be used or disclosed for a variety of purposes, such as for market research. Therefore, privacy issues occasionally arise, both from a HIPAA perspective but also in the context of other privacy laws such as state laws governing the protection of HIV/AIDS information, or mental health information, or security breach notification laws. Therefore, we work with a health plan client on integrating those different laws and guide them in

terms of which activities are permissible regarding utilization of the data that they possess. In many cases, the health plan does not obtain protected health information from the plan member in the first instance; such information is usually obtained from the treating physician or treating provider. Rather, the health plan is charged with maintaining the confidentiality of the information that it receives and making sure that the purposes for which the information is used or disclosed are permissible without an authorization. In addition to compliance with federal privacy laws, since these clients have so much information in computerized databases, it is very important for them to be aware of what the security laws are in the states in which they operate.

Working with Clients

Creating an Effective Compliance Program: Key Components

There are several key factors that we look at and advise the client to consider when creating a privacy compliance program. One is scale, because in order to be appropriate the program has to be scaled to the size and needs of the organization.

Secondly, it is important to consider the uses and disclosures of information in a day-to-day context and what required policies would be relevant to the organization. For example, if an organization deals only with the Medicare population, then even though HIPAA requires policies and procedures in the context of child abuse reporting, such procedures are not necessarily going to be pertinent to that organization.

Consequently, the development of an effective privacy compliance program entails a review of the organization and its functions, and then evaluating both in terms of scale but also in terms of substance in order to determine what measures are appropriate for an organization to implement. Compliance becomes overwhelming in an organization that has too many policies and procedures, and because an organization will be held accountable for complying with its own policies and procedures it is essential to prevent a situation in which compliance becomes impossible on the first day that the program is operationalized.

Therefore, in a small organization with budgetary restrictions, we will often recommend a compliance program that is fairly rudimentary, just to make sure that the client has the basics in place. However, other organizations such as a large academic medical center, health plan or pharmaceutical company will need a much more robust compliance program, because a host of issues could come up for such clients, and those programs need to be revisited more often because new initiatives are being employed frequently that could raise privacy issues. At the same time, we always try to be very cognizant of the business needs of the client organization and how it actually operates, because as lawyers, our work is useless if all we do is inform our client regarding what the law requires without taking into account what their operational picture looks like. We have to understand what the client's business involves in order to advise the client appropriately and assist them in establishing a workable compliance program.

Looking to the Future: Enforcement Concerns

Presently, we are seeing more enforcement activity taking place with respect to HIPAA on the federal level. On the state level, various attorneys general have been active in pursuing enforcement where there have been security breaches; therefore, this is an important area to monitor, particularly for large organizations. The FTC has also been quite active in enforcement activity regarding companies' compliance with their Web sites' privacy policies.

An increasing number of states have introduced legislation on privacy and security, and there is congressional legislation that has recently been introduced regarding privacy as it relates to electronic health information as well as regarding security breach notification. It will be very interesting to see what sorts of changes may take place in the context of privacy after the upcoming presidential election. Following the last change in administration, HIPAA Privacy Rule provisions were scaled back from the initial proposed legislation. Therefore, depending on the administration that takes office, we could see more activity in the context of privacy regulation.

Final Thoughts

I advise younger attorneys who are working as outside counsel in this practice area that it is very important to keep abreast of all the new

developments that are taking place with respect to privacy law compliance, so that your clients can also be aware of them. With respect to in-house counsel or privacy officers, it is very important to continually take stock of your organization in order to evaluate various new initiatives and whether privacy will be implicated. The involvement of such individuals in new consumer marketing initiatives, for example, is important to ensure that implementation includes adequate preparation for privacy compliance.

As mentioned earlier, taking an enterprise-wide approach to privacy compliance is very important within a health care organization. There must be communication across departments, and the privacy office must be involved in and aware of new initiatives that involve the use and disclosure of confidential health information in order to make sure that compliance with privacy and security laws remains paramount.

Linda A. Malek, a partner at Moses & Singer, chair of the Health Care practice and co-chair of the Privacy practice, focuses her practice on health care transactions, health care technology, and regulatory matters concerning the health care industry. Her work at the firm has included advising a variety of health care entities on health care transactions, including the emerging laws and regulations affecting the health insurance industry, the impact of the Medicare Modernization Act, counseling health care organizations on compliance issues related to federal, state and international privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA), drafting risk agreements for ventures involving large health maintenance organizations, structuring arrangements involving human subjects research, representing both for-profit and not-for-profit health care entities, and counseling payors, providers, and pharmaceutical companies on a variety of regulatory compliance issues, including privacy, clinical research compliance, and fraud and abuse under federal and state laws.

Prior to joining Moses & Singer, Ms. Malek spent nearly six years practicing as a health care attorney for the Office of the Corporation Counsel, Division of Legal Counsel, where she was named Outstanding Assistant Corporation Counsel by the Association of the Bar of the City of New York. Her expertise in a wide range of health care issues has included advising many types of clients on Medicare and Medicaid reimbursement issues that affect hospitals, managed care providers, mental health care providers, and New York City agencies.

Ms. Malek also has extensive experience in advising clients on issues of corporate governance and ethics in the health care environment, in counseling clients in the context of qui tam actions and the False Claims Act, and in assisting clients in establishing internal compliance programs.

Ms. Malek has authored numerous articles and publications on health care privacy topics. She attended the University of Virginia School of Law (J.D., 1993) and Walla Walla College (B.A., cum laude, 1989).

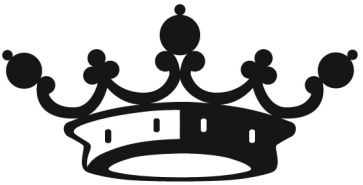
ASPATORE

www.Aspatore.com

Aspatore Books is the largest and most exclusive publisher of C-Level executives (CEO, CFO, CTO, CMO, Partner) from the world's most respected companies and law firms. Aspatore annually publishes a select group of C-Level executives from the Global 1,000, top 250 law firms (Partners & Chairs), and other leading companies of all sizes. C-Level Business Intelligence™, as conceptualized and developed by Aspatore Books, provides professionals of all levels with proven business intelligence from industry insiders – direct and unfiltered insight from those who know it best – as opposed to third-party accounts offered by unknown authors and analysts. Aspatore Books is committed to publishing an innovative line of business and legal books, those which lay forth principles and offer insights that when employed, can have a direct financial impact on the reader's business objectives, whatever they may be. In essence, Aspatore publishes critical tools – need-to-read as opposed to nice-to-read books – for all business professionals.

Inside the Minds

The critically acclaimed *Inside the Minds* series provides readers of all levels with proven business intelligence from C-Level executives (CEO, CFO, CTO, CMO, Partner) from the world's most respected companies. Each chapter is comparable to a white paper or essay and is a future-oriented look at where an industry/profession/topic is heading and the most important issues for future success. Each author has been selected based upon their experience and C-level standing within the professional community. *Inside the Minds* was conceived in order to give readers actual insights into the leading minds of business executives worldwide. Because so few books or other publications are actually written by executives in industry, *Inside the Minds* presents an unprecedented look at various industries and professions never before available.



ASPATORE

MOSES & SINGER LLP

Disclaimer

Viewing this document or contacting Moses & Singer LLP does not create an attorney-client relationship.

This document is intended as a general comment on certain recent developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This document contains timely information that may eventually be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions or matters but that professional advice be sought in connection with any such transaction or matter.

Attorney Advertising

It is possible that under the laws, rules or regulations of certain jurisdictions, this document may be construed as an advertisement or solicitation.