wiley

NEWSLETTER

HIPAA/HITECH Compliance Is Finally Here

September 2013

More than four and a half years since the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act, the time for compliance with the updated Health Insurance Portability and Accountability Act (HIPAA) rules is finally here. The health care industry has changed tremendously during this period, and there is a wide variety of new programs, technological developments, and policies to incorporate into any health care business. With this new compliance period upon us, what can we expect and what are companies likely to have missed?

This new era has been a long time coming, and despite this delay, the overwhelming percentage of changes to the HIPAA rules simply track the words of the HITECH statute. Companies affected by these changes have had four-plus years to prepare for this new environment.

Enforcement Approach

Do we expect September 23, 2013, the new compliance date, to be a significant date? Presumably, the day will pass without any noticeable events. There is no reason to think that the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is primed to pounce on compliance weaknesses starting at midnight. In fact, there is little reason to anticipate any material enforcement developments at all. HHS has had much of this four-year period to use as a basis for enhanced or expanded enforcement, given the new penalties that are implemented by HITECH (and the new administration that took over at essentially the same time). However, while enforcement has continued its slow, steady pace, we have not seen substantial changes in OCR's enforcement approach or in the kinds of enforcement actions that are being taken. HHS—particularly OCR Director Leon Rodriguez—has gone out of its way to describe an enforcement approach driven by ongoing, widespread compliance failures, not single glitches or close judgment mistakes. OCR, in particular, seems to recognize the continuing importance of reasonable sharing of information in the health care industry and good-faith efforts to meet the security rule principles. It remains committed to an "educate and fix problems" approach, not the "gotcha" approach that we see in certain other health care areas (such as the health care fraud arena). While not all enforcement cases clearly reflect this approach, the cases that have been brought to date (while still modest in volume) all appear to have reflected either repeated problems or significant failures to conduct HIPAA-required activities.

The biggest enforcement issue going forward will be how HHS will address HIPAA issues related to business associates. The expansion of the HIPAA rules to business associates is the biggest overall change from the HITECH statute. Companies that contract with HIPAA-covered entities—and the companies that are downstream contractors for these companies—all face HIPAA compliance obligations and potential enforcement. Despite the four-year preparation period, many of these business associates and downstream subcontractors are not fully prepared for HIPAA compliance. Some are still unaware of their obligations. Others face HIPAA exposure even though their use and disclosure of protected health information (PHI) is exceedingly limited—and often may even be unknown to the business (*e.g.*, a document storage company or cloud vendor that maintains all kinds of information, some of which may include PHI, without any work involving the use or disclosure of this information or any explicit knowledge that PHI is involved at all). These business associates will be complying with HIPAA in a wide variety of ways, and HHS will face a real challenge in evaluating compliance issues. If history is an indication, we can expect a reasonable approach to the overall need to meet HIPAA standards, at least for the next few years.

Industry Developments

Another important factor in the enforcement approach and the overall success of the new HIPAA rules is the significant change that has occurred in the health care industry since the HITECH law was passed. Obviously, there is much greater use of the electronic health records that were the driving force behind the HITECH law (although use has been more limited than expected, and much more expensive, and the development of health information exchanges has been slow).

At the same time, we have seen enormous technological developments in the health care industry, particularly in the form of new mobile applications for health care purposes. While many of these applications are subject to HIPAA rules, many others are not, mainly because they are distributed in a direct-to-consumer model that does not involve a HIPAA-covered entity.

These developments in mobile technology also have intersected with various policy goals related to patient engagement, as part of health care reform and otherwise. In virtually all situations, the goal of patient engagement involves more information flowing to patients from more sources. All of these activities create tensions with the detailed requirements of the HIPAA privacy and security rules.

In addition, there have been significant expansions in government health care programs as a result of the health care reform movement. Many of these new programs have implemented privacy and security requirements that go beyond HIPAA, and create tensions and complexity through differing requirements. The continuing development of health insurance exchanges may present the most ongoing tension, as these exchanges' rules extend well beyond the requirements of HIPAA, even for entities directly covered by HIPAA.

What Did Companies Likely Miss?

A few last-minute items for companies to pay attention to in their compliance efforts:

- **Business Associate Contracts.** Covered entities should be ensuring that all business associates have appropriate business associate contracts in place. While there clearly is some flexibility for revising existing agreements, based on the "transition" provisions for business associate agreements, companies should ensure that appropriate steps are being taken even now. The same principle applies to business associates with their downstream contactors—all downstream contractors that receive, access, or maintain PHI need to be subject to contract obligations.
- **Security Policies and Procedures.** The single biggest compliance challenge under the new HIPAA rules is the obligation of business associates and downstream subcontractors to comply with the entirety of the HIPAA Security Rule. This is a big deal. HHS, to date, has not been helpful in providing assistance for business associates, particularly those for whom the health care rules are a small part of a larger corporate operation. Each business associate and subcontractor will need to evaluate its compliance approach to the security rule, addressing both "good security" practices and the detailed documentation and process requirements of the HIPAA rule. While this is not a small endeavor, making sure that security practices are effective—and therefore reducing the risk of security breaches—will be the single biggest compliance step that can be taken, even if documentation lags behind implementation of effective controls.
- **Breach Notification and Investigation Issues.** Many companies are struggling to develop appropriate procedures to deal with the HIPAA breach notification rule. Confusion still reigns on the meaning of the changes to the breach notification rule, particularly the movement from "significant risk of harm" to "low probability of compromise." HHS has been clear in many of its public comments that it does not view this change as a substantial one, but there still is real confusion. For covered entities and business associates, some key points on breach investigation and notification include:
    - Make sure your people report problems quickly so that they can be investigated fast and mitigated where possible.
    - Move quickly to shut down any problems or recover any data that is subject to the breach.
    - Be aggressive and thoughtful about what kinds of risks can result from an incident.
    - Focus less on a "one-size-fits-all" process than on a flexible approach that can address the particular problem.
    - Report breaches where it is reasonable and responsible to do so—don't cut too fine a line in determining a "low probability of compromise." Err on the side of more notice rather than less.

Sale and Marketing Issues

Make sure that you have thought about the implications of the new sale and marketing provisions. They are similar, but cover very distinct areas. Make sure you have analyzed both where the HITECH changes affect your practices and where you have been engaging in practices in the past that implicate these provisions.

Stay on Top of Business Changes

In addition, it is critical for health care businesses and business associates not to become too complacent about their compliance activities. Business changes, technology changes, and policies and procedures evolve. It is critical, particularly on the security front, to stay on top of the ongoing evolution of your business. It is clear that many of the recent problems under HIPAA have stemmed from business or technology developments that have not been properly incorporated into existing compliance structures. When something changes in your business, make sure you are adapting your compliance program to the new development.

Conclusion

On the whole, while the September 23, 2013 compliance date is an important one, companies should view this as the midpoint, not the end, in implementing an overall compliance approach. It is critical to continue to review overall practices on privacy and security, to pay attention to where problems are arising and where enforcement issues are becoming more prominent and, in general, to continue to be smart about how health care information is protected across the country.