'HIPAA2' legislation means more delicate handling of data

Late last month, new rules for electronic health records came into play in the US. The changes aim to protect patient data and provide guidance on what should happen if information is stolen or accidentally released. However, although many people agree that safeguards to protect electronic records are important, some worry that the additional restrictions could inadvertently create complications for clinical research.

Although some of these new rules are just now coming into force, they were approved as part the Health Information Technology for Economic and Clinical Health Act (the so-called HITECH Act), which is Title XIII of the American Recovery and Reinvestment Act that President Obama signed into law in February 2009. The legislation extends the requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. As a result, many people have dubbed the changes set forth in the HITECH Act as 'HIPAA2'. Whereas the original HIPAA applied largely to protecting patients' paper records, "HIPAA2 takes the genesis step to electronic medical records," says Howard Asher, president and chief executive officer of Global Life Sciences, an information technology company based in San Diego.

> "Inevitably, health care will go completely to electronic health records."
> —Howard Asher

In the past, HIPAA's regulations applied primarily to physicians, hospitals and insurance providers. The new rules now also apply to business associates, which include outsourcing partners that might handle data storage, security or general information infrastructure. "HIPAA2 creates a big task for business associates, which hadn't been held—until now—to most of the HIPAA security and privacy standards," says Stanley Nachimson, principal of Nachimson Advisors.

As a result health care groups must revisit business-associate agreements, says James Kurack, a privacy and data security expert at Obermayer Rebmann Maxwell & Hippel in Philadelphia. Now, covered entities should ensure their business associates administer the appropriate safeguards to protect electronic health information and promptly report any breach of unsecured personal health information.

For example, a business associate should follow guidelines published by the US Department of Health and Human Services (HHS) for keeping data secure, such as using encryption. This way, if data get stolen, the information is more difficult to extract. If any unsecured data—meaning that it is easily readable by anyone without decoding—are released inadvertently or stolen, it might need to be reported.

According to Asher, the additional requirements for handling data, especially meeting privacy concerns, might also create a temporary obstacle for clinical researchers conducting ongoing studies on anonymized patient information. Investigators might be more reluctant than before to share such patient details with external clinical research groups for fear of data breaches. There should be no concern, however, as long as a patient's medical record was truly disassociated from the individual before entering the data in an anonymous database. As Asher explains, if pre-disassociation was in fact the case, then re-association with the individual patient is highly unlikely and indeed best practice.

Tougher penalties

HIPAA2 requires more active notification of data breaches than previous rules did. "Lots of clients are struggling with what needs to be reported," says Kurack. "Not all breaches need to be reported, only those that pose a significant risk of harm." According to HIPAA2, that risk depends on several elements, including financial or reputational harm to the individual whose personal health information was compromised. In some cases, data breaches must be reported to HHS and even the media.

Moreover, the new regulations include stiff financial penalties. For example, even an individual unknowingly violating a HIPAA2 regulation can be charged as much as $1.5 million in a year for repeat violations. HIPAA2 also gives state attorney generals the authority to investigate violations. "So, providers should expect HIPAA2 to increase the emphasis on enforcement," says Nachimson.

In the end, changes required under HIPAA2 increase the demands on anyone using electronic health records. "This is not just a vendor issue," says Nachimson. "You can't turn to whoever manages your IT and expect them to take care of everything. There are policy changes and employee training involved."

Despite the new complexity, electronic records are the future. "Inevitably, health care will go completely to electronic health records," Asher says. "The question remains: how do we do it safely and trust it?"

Mike May, Houston

Grassley probes health care technology

The US government is poised to spend billions on electronic records to help streamline health care delivery. But, after complaints that companies put all the blame of computer errors on hospitals and physicians, one rabble-rousing lawmaker is questioning the technology's efficacy.

Senator Charles Grassley, a Republican from Iowa, wrote to 31 hospitals across the country in January to investigate their experiences with health information technology, such as systems that allow physicians to enter prescriptions into a computer instead of hand-writing them. The correspondence comes only months after Grassley sent letters in October to ten companies—including medical equipment giants 3M and Philips Healthcare—inquiring about liability limitations in their contracts associated with health technology.

According to Thomas Yackel, an internist at the Oregon Health & Science University in Portland, most contracts between health care providers and makers of e-health software include wording that could be paraphrased as 'use this system on real patients at your own risk'. "Most of these contracts look like the vendors are washing their hands of any responsibility, but, to be a good vendor, you can't do that or no one works with you," says Yackel, who studies errors in health care informatics.

Tech companies echo at least some of Yackel's assessment. "In order to have a cooperative and successful relationship, we do not—and, in general, vendors should not—always put all responsibility for errors on the customer," says Irfan Iqbal, director of medical informatics at Sequel Systems, a medical software company in Melville, New York.

Mike May, Houston