

# Privacy and Security a Gordian Knot Far From Being Cut

Save to myBoK

By Lynne Thomas Gordon, MBA, RHIA, FACHE, CAE, FAHIMA, chief executive officer

Recently, the *New York Times* ran a provocative opinion piece that called for increased use of patient data for research purposes. “When I explain to my own patients what can be done with their medical information for the greater good in research, nobody has ever said to me ‘don’t use my data,’” the author, a professor of medicine, wrote.<sup>1</sup>

The article is a thought-provoking vision of the future role the public could play in important medical discoveries. But the reality is more complicated. Thirteen years after the implementation of HIPAA rules, the industry is a long way from cutting the Gordian knot that is privacy and security.

It’s important that patients trust that their information is safe, otherwise bad care or bad decision-making could result. However, the industry is struggling upstream against an onslaught of privacy and security breaches, as well as cyber attacks and patient identity theft. These events make it difficult for patients to trust.

But the long-term curve will likely bend toward more data sharing. There can be benefits to data sharing, as the Precision Medicine Initiative suggests, if the shared information is private and secure and patients are on board.

It’s a big “if.” A recent Pew Research Center study found that 52 percent of respondents would be willing to use a health records website; 26 percent were not in favor, and 20 percent answered “it depends” on the circumstances.<sup>2</sup> Given today’s confusing circumstances, such ambivalence is understandable.

Privacy and security is no less of a challenge for those on the front lines. Earlier this year, the Department of Health and Human Services proposed changes to the rule regarding how patients’ substance abuse and addiction treatment records are shared. With these and other changes, organizations must continually stay current and understand what information patients, family members, other providers, and business associates can access.

This month’s *Journal of AHIMA* looks at some of the most pressing issues related to privacy and security. In “[Release or Not?](#)” Mary Butler discusses the recent changes to release of information practices, including new and revised privacy regulations, which are becoming increasingly complex. In “[Information Governance for Offsite Data Security](#),” Devendra Saharia examines ways providers can protect data and limit exposure to attacks.

There are other ways we can improve our operations. Christine Lee defines HIM strategies and tactics for practices transitioning from physician-owned to hospital-employed in “[Bringing Physician Practices into the HIM Fold](#).”

The biggest HIM issues are also global phenomena. Lorraine Fernandes and her international co-authors offer a preview of this fall’s IFHIMA Congress in Tokyo, Japan, in “[IFHIMA Organizing a World of HIM](#).”

HIM professionals must ensure that all parties are invested in protecting and securing personal information. As the experts in this area, we are well positioned to lead the way forward.

## Notes

[1] Agus, David. “[Give Up Your Data to Cure Disease](#).” *New York Times*. February 6, 2016.

[2] Rainie, Lee and Maeve Duggan. “[Privacy and Information Sharing](#).” Pew Research Center. January 14, 2016.

### Article citation:

Gordon, Lynne Thomas. "Privacy and Security a Gordian Knot Far From Being Cut" *Journal of*

*AHIMA* 87, no.4 (April 2016): 13.

---

**Driving the Power of Knowledge**

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.