COSMOS
Navigate the Compliance Universe

Compliance Today - February 2021
Health information compliance: Building a seven-element program for the 21st Century Cures Act

By Nick Weil, JD, LLM, CHPC, CHC

Nick Weil (nick.weil@ankura.com) is Director, Data Privacy and Compliance, at Ankura Consulting, living in Omaha, NE.

- linkedin.com/in/nick-weil-0a004649

New federal rules for the healthcare industry—the information-blocking rule[1] and the interoperability rule[2] —were published May 2020.[3] Compliance was initially set for November 2020 but got delayed until April 2021.[4] The new rules were promulgated during an initiative around patient access rights by the Office for Civil Rights last year,[5] and both come on the heels of recent sea-change laws in California (California Consumer Privacy Act) and Europe (General Data Protection Regulation) that greatly expand the access and portability requirements of personal information. Indeed the two most recent federal bills—one "sponsored by Senate Democrats" and one "proposed by Senate Republicans"—proposed by Congress requiring general-industry privacy law *both* have transparency and portability requirements.[6] Add in, for good measure, the surge of public health, telehealth, and clinical research requests as care, vaccines, and cures for COVID-19 are sought, and compliance professionals should be searching for a framework for complying with information access and data governance requirements.

Duties and rights with regard to data protection, security, and privacy—contained in the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act, 42 C.F.R. § 2 , state, and other law—have been widely examined and internalized by compliance departments. Less compliance attention has been paid, on the other hand, to the duties of organizations and corresponding rights of individuals to access, share, and port those same data. In many health systems, patient rights under HIPAA are usually delegated to health information management (HIM) or medical records departments with only occasional support or oversight from compliance. Many in the healthcare space could safely ignore recent jurisdictional laws that swelled the rights of data subjects, so it might come as a surprise that individuals have the level of power over their health information that they do. The days of salutary neglect may be behind us though, because the new information-blocking rule and the 21st Century Cures Act require compliance departments to take a more active role in how electronic health information is managed, released, and accessed across the organization.

A previous *Compliance Today* article[7] examined the new rule and its requirements in detail, which will not be replicated here. Rather, we want to turn our attention to how to comply with the new rules. It might also be described as a new ethical framework, because it replaces a one-sided focus on data protection with a balance between security and portability, privacy and access. Traditional HIPAA compliance programs may be inadequately aligned to engage these new requirements and expectations, because they are often preoccupied with preventing and mitigating breaches. But using the seven elements as a guide, compliance and privacy programs can refocus with an eye on the new information-blocking rule, allowing them to lay foundations for a regulatory landscape that will increasingly emphasize the access, control, and portability of health information.

The seven elements

The new rule will be enforced by the Office of Inspector General (OIG) of the Department of Health & Human Services,[8] so what better framework to use than the OIG's own guidance on what makes an effective compliance program?[9] In this article, we will explore each of the seven elements and discuss ways that compliance programs can deploy them to meet the new rule requirements. The seven elements include: (1) policies and procedures, (2) officers and committees, (3) education and training, (4) effective lines of communication, (5) corrective action for violations, (6) auditing and monitoring, and (7) investigation and remediation.

Policies and procedures

Compliance professionals should review the organization's policies in the event of any new regulation or requirement, and information blocking is no different. The rule requires organizations to permit the access, use, and disclosure unless certain criteria or exceptions are met.[10] The exceptions include patient harm, privacy, security, and infeasibility, among others, but written policies and case-by-case documentation are required to qualify for virtually all of them. It is a good bet that new policies will need to be drafted to qualify for these exceptions. These exceptions are very restrictive and detailed, so work with your HIM, information technology, and clinical counterparts to draft and deploy these policies in a manner that carefully tracks the regulatory requirements.

Moreover, current policies should be reviewed for potential practices that will now be considered information blocking. In its preamble to the proposed rule, the Department of Health & Human Services lists several common practices that it considers to be information blocking.[11] Conspicuous among them is citing HIPAA where it does not apply or actively prohibit a disclosure. Compliance professionals should review their privacy policies and patient notices and release of information procedures to confirm they are no more restrictive to data access (even for third-party data access) than is required by federal or state law. Dust off your policies regarding patient right to access and restriction requests and make sure they are accurate and not overzealous in preventing access. Consider adding to your code of conduct a commitment to interoperability and transparency, too.

Finally in this section, and often overlooked by the compliance industry, are procedures: those not-quite-policy guidelines, standard operating procedures, and similar protocols that keep departments running consistently. Like policies, procedures that limit or restrict access to patient information must be examined to ensure there is not an information-blocking practice lurking. Procedures can be hard to find since they are not usually housed centrally like policies, so focus on those areas most likely to be on the front lines of requests. This is why it will be crucial for HIM and compliance to work very closely together, both on HIM procedures like the organization's release of information standard operating procedure and with all the other departments and silos where electronic health information is used or exchanged.

For example, to the extent permitted by their electronic medical record technology, providers will be required to open their notes to patients as soon as they are technically able to. But certain note types (e.g., psychotherapy notes) are carved out of the definition and need to be held back from portal or traditional requests.[12] Moreover, some provider notes (e.g., elder abuse records)[13] and lab results (e.g., pediatric pregnancy tests)[14] could implicate other information-blocking exceptions, to the point where providers will likely have to be able to hide those elements that might qualify. HIM or information technology will need to categorize those data elements that will be automatically withheld, but that cannot be done until clinical departments are actually surveyed to determine which note types they are using and where information-blocking sections apply. HIM or medical

records should be leveraged for their expertise in gathering and organizing a project of this scope.

Officers and committees

HIM departments will likely lead the charge on implementing the new interoperability requirements from the Cures Act. That is only natural and appropriate given the processes and technology involved, but it is important that compliance takes a seat at the table and helps guide the process. Other stakeholders will prioritize the problems and needs of operations, infrastructure, or clinical staff, so compliance should be there to make sure that commitment to fair, ethical, and legal conduct is considered as every decision is made.

While clinical and operational leadership should champion the rollout of open notes and interoperability practices, once the initiation phase is complete, oversight should rest with the traditional compliance or privacy committee. We will discuss in later sections what actions can be taken to manage and measure your compliance with the new rule, but for now, introduce the information-blocking rule and encourage feedback and oversight into how best to comply with its standards. Consider amending the job descriptions for the compliance officer or privacy officer to specifically include reference to information blocking, the same way they probably include references to HIPAA and the Stark Law.

That being said, key to effective information compliance programs will be a strong partnership with HIM or their equivalent at your organization. Compliance embodied in operations like information technology and HIM is always to be preferred over a separation, because it assists and demonstrates frontline commitment to ethical conduct.

Education and training

Workforce training is an essential tool in encouraging compliance at your organization. This is especially true for a rule like information blocking, because it reverses many preconceived notions about the access and sharing of patient information. Physicians and nurses have a healthy instinct of hyperconfidentiality drilled into them from HIPAA and doctor–patient confidentiality. But the new rule requires providers to act differently. Where before HIPAA acted like a floor, creating a minimum level of privacy protections for covered entities, information blocking has turned HIPAA into a ceiling. Remember: a practice is information blocking unless a black-letter law (or other exception) prohibits the practice. This means organizations should expect scrutiny when acting more restrictive of access—even third-party access—than privacy laws actually require.

For instance, many physician offices and hospitals are overzealous in requiring patient authorization or consent before sharing information for treatment or payment purposes. Since HIPAA permits this activity without patient authorization[15] —HIPAA *permits* the seeking of consent for treatment, payment, or operations, but the Department of Health & Human Services has commented in the preamble to the new rule that information can only be blocked if a law *requires* the practice[16] —unless some other rule prohibits the disclosure or another exception applies, that practice could be considered information blocking. Similar inferences can be drawn when family members or personal representatives make information requests of clinical staff, since HIPAA permits limited disclosures to these individuals.[17] There are dozens of other areas of the organization where information-blocking practices are likely occurring due to overreading of HIPAA or other privacy law—intentionally or not. Consider the types of procedures and conduct common in contracting, information technology, medical records, clinical research, billing, and others. Staff in these areas will need to be alerted to the new expectations around transparency of electronic health information and trained to look out for potential information-blocking practices.

Let’s look at two areas in particular from the clinical perspective: behavioral health and pediatric medicine.

Already thorny with regard to regulatory and legal concerns, these become a tangled briar within the information-blocking framework. Providers in these areas often feel the need to hold back information to prevent harm or maintain the privacy of their patients. The question becomes this: When can a provider block information access by a mental health patient or a parental proxy? These providers usually have nuanced processes for dealing with mental health notes or self-consenting minors under state law. Information blocking is liable to be the wrench thrown into those delicate processes. Be sure that staff in these specialties and departments are aware of this new rule, the exceptions, and receive training on its requirements. More broadly, your organization-wide compliance training should be updated accordingly as well.

Effective communication

This section of the OIG elements is reserved for the anonymous hotline and other avenues to encourage reporting and resolution of issues. This requirement is no different under an information-blocking compliance program. See that your hotline notices, postings, websites, and instructions to reporters include reference to information blocking as a reportable issue. This will be key, not only to driving compliance, but also to heading off potential issues before the OIG receives them. If not already available to the public, ensure that the compliance line is public facing; information-blocking reports are just as likely to come from patients and other third parties as they are from staff.

Disciplinary actions

Like every other federal regulatory requirement, the OIG will expect organizations to take disciplinary action against employees who violate the information-blocking rule. This does not mean you should throw the book at the first doctor who blocks patient access that does not completely qualify for the harm exception, or terminate an HIM specialist who inappropriately denies access under the new rule, but it does mean information blocking should be addressed in your compliance sanction policy and procedure. Not only do violations threaten the organization with fines and penalties, they are also bad for the patients. This article is not the place to discuss the public policy aims and merits behind information blocking and open notes, but a lot of good research (e.g., OpenNotes.org, a nonprofit partnership of providers and public policy experts, conducts and distributes regular clinical research, studies, and resources on health information interoperability) has been done about the benefits of greater access and transparency into medical information. Keep this in mind when enforcing the information-blocking rule.

Auditing and monitoring

Earlier we discussed how organizations will likely have to deploy a process where a provider can block or hide a specific note from automatic patient portal access in the event of harm, or privacy, or another exception being applicable. A number of the information-blocking exceptions specifically call for professional caregiver judgment. This level of individual determination has a high potential for error and abuse. Work with your HIM department to produce reports through your electronic medical records that can track and trend which providers are denying access. Outliers or heavy-use departments should be targeted with additional training and enforcement as needed.

Additionally, audit your HIM or medical records department to determine if they are following the new policies and procedures. Sample a number of patient access requests and determine whether they were honored in compliance with the information-blocking rule. If you use a HIPAA walk-through or on-site privacy survey process, add a question related to information blocking and see how staff respond. If your program does not already have such a walk-through, deploy one now that addresses privacy and information-blocking requirements.

Investigation and remediation

The seventh element of an effective compliance program is investigation and remediation.[18] Be sure to take complaints of information blocking seriously and investigate them like you would any other compliance allegation. Give priority to those instances that cause patient harm, significantly affect treatment, cause financial loss, or are performed with actual knowledge or for long durations; these are what the OIG indicated it would prioritize.[19] It would not hurt to do the same.

Once an investigation is completed and corrective action with the offender is performed, review what broader remediation might be appropriate. Most often, a given compliance violation does not happen because someone woke up one day deciding to break the law. Systemic issues or procedures, pressures, or incentives caused the conduct. Review these seven elements after the first couple of investigations to determine whether additional policies, trainings, or audits are appropriate to address the root cause.

The 8th element and conclusion

The risk assessment has been sometimes called the unofficial eighth element of an effective compliance program. Ideally before the compliance date (but at the latest soon thereafter), compliance should conduct or contract a readiness assessment for information-blocking compliance. These rules are very complicated and sprawl across the health industry in unexpected ways. It helps to have an independent set of eyes (whether compliance, internal audit, or a third party) review how ready your organization is to comply with the new rule. An important pillar of compliance is that whoever operates should not audit, because it is not possible to assess your own work product without some degree of bias and conflict.

It goes without saying that healthcare has a lot on its plate at the moment. It can be hard to justify another onerous regulatory regime in a time of a worldwide pandemic and economic uncertainty. Against such concerns, it is important to cite, as we did above, the great benefits of interoperability and open notes. Healthcare in such times is more necessary, not less, and so it is more necessary than ever that patients and family trust their healthcare providers and their health information managers. The best way to earn trust is to be open and transparent, and health information compliance can help organizations do just that. Conceiving health information as an integral area of compliance will also position your organization to comply with new laws, both in the near term as represented by the information-blocking rule and in the long view.[20]

Takeaways

- The information-blocking rule requires compliance programs to refocus on health information access and portability as a potential area of risk.
- Professionals should review their Health Insurance Portability and Accountability Act policies and procedures to ensure they are updated for the new requirements.
- The new rule cuts against a lot of healthcare provider confidentiality instincts, so staff will need to be retrained.
- Partner with health information management and information technology departments to quickly and thoroughly review and prepare your organization for the compliance date.
- Review the seven elements of an effective compliance program from an information-blocking rule perspective.

145 C.F.R. § 171 .
245 C.F.R. § 170 .
3 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25,642 (May 1, 2020) , https://bit.ly/32vJ6RI.
4 U.S. Department of Health & Human Services, "HHS Extends Compliance Dates for Information Blocking and Health IT Certification Requirements in 21st Century Cures Act Final Rule," news release, October 29, 2020, https://bit.ly/34PyspD.
5 "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524 ," U.S. Department of Health & Human Services, last reviewed January 31, 2020, http://bit.ly/3cJ7iTf.
6 Wendy Zhang, "Comprehensive Federal Privacy Law Still Pending," *The National Law Review* X, no. 22, January 22, 2020, https://bit.ly/2K7o1WS.
7 Josh D. Mast and Cheri Whalen, "Ten compliance concerns related to information blocking," *Compliance Today*, January 2021.
842 U.S.C. § 300jj-52(b) .
9 Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8,987, 8,989 (February 23, 1998) , http://bit.ly/2Mfc9B9.
10 "Information Blocking," Office of the National Coordinator for Health Information Technology, last reviewed November 23, 2020, https://bit.ly/2ZjCioP.
11 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program 84 Fed. Reg. 7,424, 7,518 (March 4, 2019) , https://bit.ly/3mq9lQ4.
1245 C.F.R. § 171.102 .
1345 C.F.R. § 171.201 .
1445 C.F.R. § 171.202 .
1542 C.F.R. § 164.506(b) .
16 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25,845 .
1742 C.F.R. § 164.510(b) .
18 Department of Health & Human Services, Office of Inspector General, Health Care Fraud Prevention and Enforcement Action Teams, "Health Care Compliance Program Tips," last accessed July 2, 2020, https://bit.ly/3gm8ddk.
19 U.S. Department of Health & Human Services, Office of Inspector General, "OIG proposes rule for civil money penalties for information blocking," news release, last accessed December 14, 2020, https://bit.ly/384Y02p.
20 U.S. Department of Health & Human Services, Office for Civil Rights, "HHS Proposes Modifications to the HIPAA Privacy Rule to Empower Patients, Improve Coordinated Care, and Reduce Regulatory Burdens," news release, December 10, 2020, http://bit.ly/3p4xFst.