Security and Compliance in New World of Care

RICOH
imagine. change.

Prepare for Secure Information Exchange in the New World of Care

The U.S. leads other developed countries in the use of electronic health records, yet "information blocking" has undermined EHR effectiveness by inhibiting our ability to share this information.[1] Earlier this year, the Department of Health and Human Services' national coordinator for health IT petitioned Congress to help put an end to information blocking.[2] Though nearly all U.S. hospitals (97 percent) and three-quarters of physicians report possession of certified EHR technology, health information exchange remains relatively low. In fact, less than half of physicians report sharing patient health information electronically and only one-quarter (26 percent) report sharing patient health information electronically with outside providers.[3]

Though in some cases information blocking is intentional, giving hospitals or companies a competitive advantage, it is more often the result of a conservative approach to data management. Many health systems and physicians are concerned they would violate HIPAA law when sharing patient information externally. This inadvertent information blocking hinders healthcare leaders' ability to best serve patient populations because data is trapped.

The healthcare industry has come a long way in its digitization, and now the end of information blocking is here. With mandatory data exchange on the horizon, the ability to securely capture, transform and manage information is critical.

Here are three trends to watch out for in today's world of care, along with ways you can act now to stay ahead of the security and compliance curve:

1 Focus is shifting towards outcomes, value-based care.

Merit-based Incentive Payment System (MIPS) and the Advanced Alternative Payment Model (APM) are replacing Meaningful Use programs. This shift is designed to align population health management and value based care goals, resulting in improved efficiencies, better outcomes and a more holistic view of the organization's patients and performance.

Though Meaningful Use helped the U.S. healthcare industry digitize, it also resulted in many frustrations and burdensome requirements for providers. The next iteration, mainly MIPS and APM, will focus less on technology and more on outcomes.

Central to outcomes-driven care is secure information exchange. Physicians require real-time data to make more informed care decisions. Now, patient information must not only be digital, but also accessible. It's this very accessibility that causes security concerns for physicians and healthcare IT professionals, resulting in information blocking. In fact, data privacy and security needs often seem to compete against organizational priorities like information exchange.

[1] http://fedscoop.com/onc-congress-needed-to-fight-health-info-blocking
[2] http://fedscoop.com/onc-congress-needed-to-fight-health-info-blocking
[3] http://dashboard.healthit.gov/report-to-congress/2015-update-adoption-health-information-technology-executive-summary.php

Act Now:

- Perform an information-centric risk assessment. Learn where information is flowing across your enterprise so you can best protect it.
- Take control in today's sharing culture. Instead of safeguarding information by restricting access, implement secure solutions like multi-folder sync and embedded share links, which you can monitor from within your organization.

2 Interoperability is inevitable and clean data is key.

As MIPS and APM take center stage, interoperability is no longer wishful thinking for the future. This gives way to the opportunity to thrive in today's new world of care by implementing solutions that let you share patient information across the care continuum.

For interoperability success, it's important to normalize and cleanse data. This helps hospitals, health systems and IDNs to compare apples-to-apples data when making care decisions. 'Clean' data is not only important for treatment plans and population health management, it will also help protect your organization from potential hacks.

According to information security experts, protected health information (PHI) attacks are relatively low-risk from the criminal's perspective, as they can achieve potentially large pay-offs with simple tactics. This is largely because IT cleanliness is not ingrained in healthcare.[4]

Act Now:

- Employ technology and strategies to help information travel from one EHR to another. Regularly normalizing and cleansing your data will prevent miscommunication and bolster information security.
- Consider joining a secure interoperability framework, which enables safe, clean data sharing among a large network of healthcare delivery organizations.

3 Patient data capture is coming – from nearly endless sources.

Healthcare consumerism is on the rise and patients are monitoring their health with both clinician-prescribed and patient-acquired devices. This increase in patient data capture and patient engagement will require information to not only flow between physicians and health systems, but also to and from the patients themselves.

Shipments of wearable devices for fitness are expected to reach 109.4 million units in 2017 and 129.6 million in 2018.[5] Patient data capture will become increasingly common, yet the startups targeting this market are often focused on business growth and don't make compliance a priority.

Act Now:

- Establish a secure patient portal so you can acquire patient-captured data and information on your own server.
- Before integrating with patient-acquired devices, research the manufacturer's liability and explore any necessary business associate agreements. While innovative partnerships are important, be sure to protect yourself from any vulnerabilities that these partnerships could expose.

New regulations and technologies are changing the way providers access and share information. To meet important interoperability and value-based care goals, information should be able to flow freely – and securely – between physicians, health systems and patients. Having the right security processes and technologies in place to address this new world of care ultimately helps lead to increased provider satisfaction and better care for patients.

To learn more about secure information exchange, visit https://www.ricoh-usa.com/healthcare.

[4] https://www.healthcareitnews.com/news/healthcare-enters-new-cybersecurity-era-hacktivists-organized-crime-foreign-nationals-take-aim

[5] https://www.internethealthmanagement.com/2016/08/15/philips-new-wearables-can-provide-docs-range-patient-data/

RICOH
imagine. change.

www.ricoh-usa.com/healthcare

Ricoh USA, Inc., 70 Valley Stream Parkway, Malvern, PA 19355, 1-800-63-RICOH

The content of this document, and the appearance, features and specifications of Ricoh products and services are subject to change from time to time without notice. Products are shown with optional features. While care has been taken to ensure the accuracy of this information, Ricoh makes no representation or warranties about the accuracy, completeness or adequacy of the information contained herein, and shall not be liable for any errors or omissions in these materials. Actual results will vary depending upon use of the products and services, and the conditions and factors affecting performance. The only warranties for Ricoh products and services are as set forth in the express warranty statements accompanying them.