COSMOS
Navigate the Compliance Universe

Compliance Today - March 2024

Shannon Smith (shannon@onna.com, linkedin.com/in/rshannonsmith/) is the Chief Technology Officer at Onna Technologies Inc.

How healthcare compliance professionals can prepare their data for litigation

by Shannon Smith

Every day, advancing technology—including telemedicine, wearable devices, and artificial intelligence (AI)—reshapes patient care. These new tools generate new forms of data, which—when combined with automated processes and paperless environments—make daily operations more efficient. But there's a downside: healthcare organizations are now creating and storing so much data that they can easily become overwhelmed by the data challenges of litigation.

Those challenges are apparent early on—in the discovery phase—when parties on both sides have to identify, organize, and share information that may be relevant to the issues in dispute. Healthcare compliance professionals need to know how to manage various complex forms of data, track the locations in which that data is created and stored, and consolidate information across data silos. If compliance and legal teams cannot find a way to manage these challenges, they may put their organizations at a severe disadvantage in the rest of the litigation matter. Failing to comply with the mandates of discovery can lead to costly consequences, including fines and other sanctions.

Healthcare compliance professionals need to ensure that their organizations have the right data governance and litigation readiness strategies and tools to organize their data, integrate new data from emerging technologies, and comply with data privacy and security mandates. So, we've assembled a list of questions you can ask to gauge your organization's preparedness for the data-related challenges of litigation.

Do you have a comprehensive inventory of your organization's data?

Knowing what data exists within a healthcare organization is a crucial step in litigation preparedness for healthcare compliance professionals. Potential data includes patient records, diagnostic data, billing information, and any other relevant patient or customer information, whether in electronic or hard-copy form. To respond to legal inquiries quickly and effectively, you must thoroughly understand the types of data your organization maintains and where that data is stored.

What data does your organization collect or generate?

First, inventory all known data sources in your organization to learn about your data. Start with your electronic health record systems, databases, communication platforms, and any other applications your employees use to capture or store healthcare information. Document the variety and formats of data created or captured by each data source, distinguishing between structured data (organized in databases and the like) and unstructured data ("freeform" data in clinical notes, emails, and so on).

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

Work with the data owners in different departments to further understand your data. Ask what applications they use, why they collect each type of data, and how they store and interact with the data they create or collect. Engage the IT department to understand the technical infrastructure, databases, and systems used. Be on the lookout for shadow IT—unsanctioned applications that individuals or teams may use to create data without IT's knowledge. Also, ask how departments share data with third parties, including cloud service providers, software vendors, and any other partners involved in handling healthcare data.

Together, this knowledge forms the foundation you'll use to prepare your organization for potential legal challenges—but knowing what data you have is only the first part of a data inventory.

Where is your data stored?

As you learn about the types of data your organization generates, you'll also want to ask where that data is stored. Work with data owners and IT teams to understand your organization's technical infrastructure. For example, what servers, databases, and storage solutions do you use? Is that storage on premises or in the cloud?

Take an inventory of all devices in use, including computers, tablets, and smartphones. Determine whether users store sensitive data locally on these devices or in cloud platforms. If data is stored in the cloud, ask what service providers you're working with and what security measures are in place to protect each type of data. Inquire about collaboration tools, file-sharing platforms, and other systems where healthcare data may be exchanged. Then, review your contracts and service-level agreements with each service provider to determine your access and ownership rights to cloud-based data and where that data is stored to ensure compliance with data privacy regulations.

Take these same steps with other third-party vendors and service providers. If your organization uses external data storage or processing services, learn where these third parties store and manage data. Ascertaining the location of your data is essential for compliance with data protection and privacy regulations.

Next, evaluate backup and archiving practices to identify where historical or redundant data is stored. And don't forget about hard-copy data that may be tucked away in file cabinets or warehouses. Understanding storage and backup practices is crucial for data recovery and ensuring that all relevant information is readily accessible during legal proceedings or compliance audits.

You may need to work back and forth across these initial questions several times as you identify additional data sources and build a comprehensive inventory of your organization's data. Once you have that inventory, you can begin classifying that data according to its risk level and overall value or potential relevance to litigation or compliance matters.

This document is only available to members. Please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.