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).

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.

How are you managing the risks posed by each type of data?

Compliance professionals must assess each type of data their organizations manage to determine whether it triggers legal and regulatory concerns such as data privacy mandates, HIPAA requirements, or other laws and regulations. For instance, if data contains protected health information (PHI) about patients, you must ensure that your organization takes the appropriate administrative, technical, and physical steps to protect that data. You also must ensure that all your business associates—law firms, eDiscovery vendors, and other third parties with access to data—do the same.

Do you have an efficient way to sort your data into functional categories?

Given the proliferation of healthcare data, you likely won't be able to pore over every bit and byte manually.

That's especially true when data is generated and managed across a series of disparate systems, many of which store data in different formats that don't integrate with each other. Fortunately, technology offers ways to efficiently assess data and sort it according to its sensitivity and importance.

Some eDiscovery software platforms offer real-time access to data in a centralized repository, providing a comprehensive view of all data assets. Advanced software platforms powered by AI can give you the additional "set of eyes" you need to understand documents quickly without engaging in a screen-by-screen or page-by-page manual review. These tools can connect with a variety of data sources through third-party application programming interfaces that enable you to download your data. The ingested data then undergoes a series of processes, including these:

- **Optical character recognition**: Transforms images of text documents into machine-readable text
- **Language detection:** Determines the languages used in each document
- **Entity extraction**: Identifies and sorts entities based on their names or other identifiers, including individuals, companies, and locations, and recognizes unique identifiers such as email addresses, dates of birth, mailing addresses, and Social Security numbers
- **Object detection**: Detects identification cards and passports within images
- **Summarization**: Creates a brief paragraph summarizing the content for each result on the search results page
- **Classification**: Classifies documents according to their risk profile and substance

Once data has gone through this tech-enabled assessment, you'll have a better handle on the sensitivity and criticality of each type of data. You can then sort data into different buckets based on whether it includes public information, confidential information, and/or sensitive for internal use only. This classification can help you prioritize which data you secure and manage first based on its significance and the potential risks associated with its exposure.

What measures do you employ to ensure data security and privacy?

Now that you know what types of data you have, check to see whether you are protecting it adequately.

For example, within the sensitive data bucket, you'll need to monitor for potential data privacy and protection concerns. Under HIPAA, you must ensure that third-party vendors—including eDiscovery vendors—follow strict protocols to safeguard any shared data. Although HIPAA regulations permit organizations to share information for litigation as part of their healthcare operations, they must take reasonable steps to limit disclosures to the minimum necessary scope to accomplish the intended purpose.

Similarly, if you collect or store the personal data of EU or California residents, you may be subject to the General Data Protection Regulation or the California Consumer Privacy Act. For each, you will need to assess what relevant identifying information you possess so you can be prepared to respond to individual requests for access to personal data. You will also want to ensure that you keep this data only so long as necessary to serve a business purpose.

You will likely benefit from conducting a risk-benefit analysis. Consider the potential impact of each type of data on the organization. What are the legal implications of having that data? What are the risks, including reputational? What are the benefits of having that information available?

Let's now turn from general data management considerations to a few more specific questions you can use to streamline your eDiscovery processes.

How do you identify and target relevant data for targeted, safe extraction?

Not all data is relevant to every legal proceeding. The goal of eDiscovery is to prioritize extracting information that is likely to contribute to resolving the dispute or building a comprehensive and defensible case. To do this, you'll need to weigh the data's value against the risks you previously evaluated.

Narrow the universe of potential data by focusing only on the involved parties or data types in question and limiting your inquiry to the appropriate time frame based on when the events or actions in question occurred. Specialized tools and software can facilitate targeted extraction of important data using filter criteria such as date ranges, specific categories, and other identifiers. This enables you to extract only the relevant subset of data while maintaining the overall integrity of the data set.

Targeting also limits the sensitive and confidential data you may need to protect. If sensitive data exists in otherwise responsive documents, comply with HIPAA requirements to disclose only the minimum necessary by using redaction tools to protect any additional sensitive data that is not relevant. You may need to have the legal team ask the court for a protective order to limit the number of people given access to the information.

Within your targeted data set, evaluate the potential impact and significance of each piece or type of data. Consider the legal implications and the weight each data point carries in supporting or refuting the claims at issue and assess whether the data aligns with your legal strategy. Prioritize data that directly supports or disproves claims, addresses disputed legal issues, or provides context to the overall situation. Then, apply the proportionality principle, assessing whether the effort and resources required for data extraction are proportionate to the potential value the data brings to the case.

Avoid the unnecessary extraction of data that may not significantly impact the outcome. Watch out for outdated or redundant information; use technology to flag old data and duplicate content that you don't need to waste time collecting.

Will your extraction processes damage the integrity of your overall data?

As you extract healthcare data for use in litigation, ensure that you maintain the integrity of the extracted data and the overall data set. This involves carefully selecting and implementing extraction methods that preserve your data's authenticity and reliability.

You must maintain a chain of custody for the extracted data throughout the process. Document your decision-making processes as you go, detailing why you chose specific data for extraction and any legal or regulatory compliance considerations you weighed. Then, document every step of the extraction process, including who performed the extraction, when it occurred, and what, if any, changes were made to the data. A well-documented chain of custody enhances the credibility and admissibility of the extracted data in legal proceedings.

Remember that for each software vendor you work with, you must enter a HIPAA-compliant business associate agreement that outlines the parties' rights and responsibilities with respect to the privacy and security of PHI.

Do you have the right processes in place to manage your data?

Concerned that you can't answer some of these questions quickly enough to comply with a litigation timeline? You need processes for managing your data on an ongoing basis and promptly preserving data that may be relevant to litigation.

Don't wait until you receive a copy of a complaint from an opposing party or learn that a dispute is brewing to think about how you'll manage your data in a litigation matter. Instead, start preparing for legal and regulatory proceedings today by getting to know your data and learning how to control it. By implementing a proactive data governance initiative, you'll ensure you have access to the right information at the right time.

Strong data governance doesn't just help you manage your information so you can meet discovery obligations. It also enables you to save on data storage by disposing of outdated or redundant data, detecting and avoiding potential risks lurking in your data, and raising the value of the data you keep.

To optimize your processes, you'll want to establish policies for records retention and legal holds at a minimum.

Establishing a records retention policy and a retention schedule

Creating a records retention policy and implementing a retention schedule are critical aspects of information management for healthcare organizations. A well-defined policy helps ensure compliance with regulatory requirements, facilitates efficient recordkeeping, and mitigates legal and operational risks. A clear retention schedule defines exactly how that policy will be implemented for each type of data.

Together, your records retention program ensures that you keep only the information necessary for your organization's operations. It eliminates redundant, obsolete, and trivial data that serves no business use, freeing up resources, lowering the cost of data storage, improving system performance, reducing security risks, and improving compliance with data protection regulations and privacy laws that require organizations to retain data only for specified periods and purposes.

Here are a few steps that will help you develop your records retention program:

- Collaborate with legal, compliance, IT, records management, and department heads to ensure the retention policy addresses the needs and concerns of all relevant departments.
- Build an inventory of the information your organization creates and stores, such as patient records, administrative documents, financial records, and HR documents.
- Work with your legal team to determine if the jurisdictions and healthcare sectors you operate in dictate how long you must retain certain types of records.
- Establish specific retention periods for each category of record. Consider factors such as regulatory requirements, business needs, and historical value when determining how long to keep each type of record.
- Determine appropriate methods for destructing or disposing of records at the end of their retention periods. Some records may need to be securely shredded or destroyed, while others may be permanently archived. Ensure that the methods you choose align with applicable privacy and security requirements. Maintain a comprehensive log of document destruction activities, documenting the method and details of each record disposal.
- Include details on the retention periods for each record category and the methods for destruction or archiving. Your retention program should clearly outline the purpose, scope, responsibilities, and procedures you'll use to manage records retention and disposal.
- Offer training and awareness programs to ensure that all employees understand their roles in adhering to your policy and send out regular reminders to follow its terms.
- Assess the effectiveness of your records retention program periodically, ensuring that destruction

processes are being followed. Address any discrepancies you find and adjust your policy and schedule as necessary to avoid further discrepancies and adapt to regulatory changes.

Creating a legal hold policy and implementing tools to streamline legal holds

If you're involved in a legal proceeding, you're expected to preserve information that may be relevant to resolving the dispute so it can be used at trial—and so is your opponent. A legal hold policy establishes a systematic and defensible approach to preserving data, preventing the unintentional deletion or alteration of data. That reduces the risk that you'll face a claim of spoliation—an allegation that your organization intentionally destroyed, altered, or concealed evidence.

Compliance should work closely with the legal team to establish a robust legal hold policy, starting with at least the following steps:

- Define the events or circumstances that trigger the initiation of a legal hold. These events include but are not limited to receiving a complaint or demand letter or starting an investigation.
- Establish clear communication protocols for issuing and releasing legal holds. Define when and how the legal hold team will communicate with affected employees, including instructions for preserving data and responding to legal hold notices. Communication should be timely, clear, and well-documented.
- Work with your IT team to define processes for preserving different types of data, including electronic health records, emails, documents, and other relevant information. Ensure that IT understands that it must suspend all automatic deletion processes for data subject to a legal hold and that relevant personnel know how to suspend those processes.
- Develop procedures for documenting all aspects of the legal hold process to improve legal defensibility. Create a template for legal hold notices, maintain records of communications with data custodians, and record steps taken to preserve data at a minimum.
- Consider whether to implement a legal hold software solution to eliminate some of the manual and fragmented processes that contribute to errors and oversights. Depending on your organization's size, data volume, and budget, software may be a worthwhile investment to streamline the process of notifying custodians of holds and releasing them from their preservation obligations. Software can also help you preserve data at its source to simplify data management and reduce risk.
- Communicate the legal hold policy to all relevant stakeholders and distribute it throughout the organization. Conduct training sessions to educate employees on their responsibilities during a legal hold. Ensure that employees understand what a legal hold notice is, why they must comply with it, and what actions they should take upon receiving one.
- Review and update your legal hold policy regularly to ensure it remains aligned with evolving legal and regulatory landscapes. Incorporate lessons learned from past legal hold experiences to enhance the effectiveness of the policy.

Conclusion

As healthcare compliance professionals grapple with the challenges posed by evolving technology and the increasing reliance on data, proactive preparation for potential litigation becomes paramount. By addressing these fundamental questions and implementing effective data governance practices, compliance teams can confidently navigate data-related challenges, ensure HIPAA compliance, and strengthen their litigation posture

—well before a lawsuit is filed.

Takeaways

- A solid information governance strategy—including a records retention program and a legal hold policy—is the foundation for effective litigation preparation.
- Being prepared for future litigation requires knowing your data. Inventory your data sources by working with data owners and your IT team.
- Learn where all your data—electronic and hard copy—is located. Determine what steps you'll need to take to access it.
- Identify any hidden risks in your data that may trigger privacy and security concerns under HIPAA and applicable data protection statutes.
- Use technology to streamline the processes of identifying, collecting, and preserving data for litigation while maintaining compliance with data privacy and other regulations.