opentext™

eBOOK

Legal holds without the headaches

What IT needs to know to master legal holds and preserve data for litigation and investigations

opentext™

Content

opentext™

Legal holds and why they matter

Organizations deal with lawsuits all the time. Conflicts arise over workplace discrimination, overtime pay, customer injuries sustained on-premises, intellectual property, contracts and more. You name it, someone has filed a lawsuit over it. To resolve claims, organizations need proof of who said or did what.

Today, that evidence is largely digital, and includes email, Microsoft® Word® documents, sales-tracking data, spreadsheets and databases and, increasingly, data from new sources, such as Internet of Things devices, drones, telemetric devices and more.

Organizations need to locate potential evidence and keep it safe to ensure it is available for use in court anytime litigation becomes reasonably likely. This is called **preservation of information**. One of the most important ways that companies preserve data is by implementing **legal holds**, also known as litigation holds, which notify the individuals in charge of data that they must retain it.

Legal departments cannot manage data preservation or legal holds without IT's help to gather and store information that will be needed to prove or defend a case correctly. This eBook explores the basics IT needs to know and provides tips and tricks, helpful methods and technologies to assist.

opentext™

Terminology

Electronically stored information (ESI): ESI is what lawyers call any information that is stored electronically, such as data, files and text messages.

Data custodian: The person that manages a particular category or subset of data, e.g., each employee is the custodian for his or her own email and documents.

Data steward: Anyone in the IT or records management department that controls data or manages its deletion or storage.

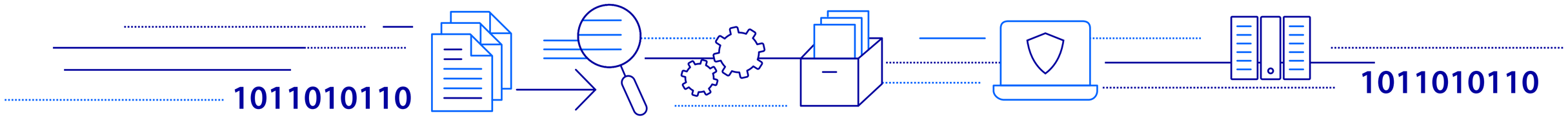
Preservation: The process of safely maintaining ESI from the time that litigation becomes reasonably likely until the matter is concluded, as determined by legal.

Legal hold notice: A communication directed to data custodians that informs them of their duty to preserve ESI for potential litigation. The legal hold notice should tell custodians what data is potentially relevant and what they should do to preserve that evidence.

Collection: The process of extracting potentially relevant ESI from its source and maintaining it in a secure storage site during litigation. Some data can be "preserved in place," or protected within its native source, so that it does not need to be collected in a secondary location.

Spoliation: The irreplaceable loss of ESI due to intentional deletion, poor preservation or, sometimes, unforeseen or accidental events. Note: If ESI can be obtained from another source, it may be lost from one source without spoliation.

Chain of custody: Documentation of everything that has happened to data during a case, including what type of data it is, when it was collected, how it was collected and by whom. If evidence is challenged in court, the chain of custody is how legal proves that it was not modified or tampered with.



opentext™

Roles of legal and IT

Legal is responsible for most of the planning and decision-making involving legal holds. That leaves IT responsible for providing information to aid legal in defining the scope of data needed for a matter and executing technical tasks. IT can expect to play a significant role in or take the lead on:

- Identifying data custodians that could have relevant data or knowledge.
- Identifying data sources and data types.
- Ensuring automated IT tasks are appropriately managed, such as suspending standard data retention and deletion practices.
- Collecting data or ensuring that it is preserved in place.

IT should plan to work in concert with legal to develop reasonable data collection protocols for different types of data. It is important to discuss the chain of custody and what documentation will be needed before executing on those protocols.

There are two additional points to be aware of. First, when a duty to preserve ESI has attached, time is of the essence. Legal must be able to issue a legal hold notice, and IT must be prepared to act on it immediately. Second, courts require counsel to supervise legal holds and data collection. If lawyers are asking a lot of questions about a hold or specific data, it is not a sign of mistrust. They are doing their job.

If information is not preserved correctly, the consequences can be severe: Courts can impose monetary sanctions, instruct the jury about the lost evidence and what it might have said or even throw out an entire case.

opentext™

Key steps

Step 1: Identify the trigger event and locate relevant data

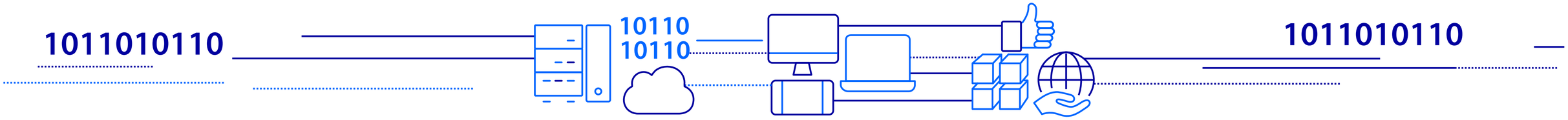
For an organization to issue a legal hold or start preserving data, it needs to know that litigation is reasonably likely to occur. Litigation might be reasonably anticipated when:

- An employee files a formal complaint of workplace harassment or discrimination.
- An employee is seriously injured on the job.
- A contract for goods or services falls through.

Identifying the trigger event that obligates an organization to start preserving data is up to the legal department, not IT.

Once legal has notified IT that an obligation to preserve data for a potential litigation matter has attached, the teams should work together to quickly determine what data should be preserved. Discuss with legal what data custodians or stewards might have relevant information, who is involved in the matter and who might have information about the underlying facts. If a custodian is accused of wrongdoing, determine how to put a hold on their data, ensuring that it cannot be deleted or modified. Sometimes, this will be done without their knowledge.

Be sure to look at every type and source of data that the organization generates or maintains. Proactively advise legal about data that they may not be aware of, especially from newer sources, such as keycard logs, security camera footage or collaboration application data.



Step 2: Issue and monitor legal hold notices

Once data custodians and the types of data that need to be preserved are determined, the legal department will issue a legal hold notice. Individual custodians will be told not to delete or modify their own data. Legal hold notices issued to the IT department might direct IT to suspend routine document destruction policies, implement a silent hold on a custodian's data or collect specific data into a separate repository.

The legal department should ask all legal hold recipients to acknowledge that they received the hold notice and confirm that they are complying with its terms. Legal should also distribute periodic reminders so that data custodians know what data is still subject to a legal hold. This is especially helpful for custodians who manage multiple concurrent holds. Be forewarned: Litigation can go on for years and holds last the entire time.

Fortunately, technology can streamline and simplify the entire legal hold process from original issuance of a hold through tracking acknowledgments and sending automated reminders. OpenText™ Legal Hold allows users to quickly and efficiently issue legal hold notices and effortlessly track responses, questions and answers, acknowledgments and reminders, making it simple to demonstrate to a court exactly what reasonable steps the organization took to preserve data.

Step 3: Collect and preserve data

At this point, legal has advised data custodians about their obligation to preserve data and IT has suspended routine destruction policies for affected data and perhaps implemented automatic preservation wherever possible. Now, it is time to collect ESI so it will be available for the legal staff to use in litigation and provide to an opponent in discovery.

It is absolutely critical to maintain the integrity of all collected data to avoid any alteration or loss of data, including both the data within the files and its metadata.

Collection tools, such as OpenText™ EnCase™ eDiscovery, can safely and securely collect data from custodians anywhere in the world, directly through enterprise email, networked drives or cloud storage repositories, using forensically sound and defensible collection methods.

opentext™

Document everything

If lawyers cannot prove something in court, it might as well not have happened at all. That is why lawyers insist that everything, from initial selection of data custodians through each step of data collection, processing and production, be meticulously documented.

Remember that legal may be called on to establish the chain of custody for any piece of data. This is how legal proves that the collected data is, in fact, the original data and has not been altered, tampered with, updated or massaged into something more favorable.

There is another reason to document everything. Should data somehow be lost through a system failure, a natural disaster or sheer mistake, the only way legal can defend against a claim that the organization intentionally deleted data is by producing a full record of everything that was done to identify, gather and preserve ESI for the litigation. Documentation is the ammunition that legal needs to prove that the organization took reasonable steps to preserve data.

opentext™

Collaboration tips

Legal holds require careful coordination and smooth collaboration between legal and IT. Here are a few guidelines to work together to better manage legal holds.

1. Start by investigating what the litigation is about in layman's terms, including any defenses the organization might have in this discussion. Brainstorm what types of data could be helpful and which custodians are likely to have that data.
2. Determine where relevant ESI might be located. If there is an organizational data map, now is the time to use it. Be sure to consider newer data sources, such as personal cell phones, social media accounts, collaboration tools and instant messaging applications.
3. Work with legal to develop a realistic collection strategy and timetable that spells out what individual custodians, other data stewards and IT staff will do to collect and manage ESI. EnCase eDiscovery can ensure that data collection is forensically sound and legally defensible.
4. If the organization uses a manual legal hold notification process, research available commercial software that can manage the legal hold process. Software, such as OpenText Legal Hold, will not only issue legal holds more quickly and monitor them more efficiently but also provide an organization with a much more defensible process.
5. Think ahead to the end of the matter. Talk with legal to understand how to know when the matter has concluded, how to return collected data to the standard record retention cycle and how data that has been distributed to outside counsel, expert witnesses or opponents will be recovered.

Discover how OpenText Legal Hold helps law departments comply with legal hold obligations, be more efficient and automate time-consuming and risky manual processes.

Learn more »

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

opentext.com

Twitter | LinkedIn | CEO Blog