VERITAS

Healthcare: Regulatory Compliance Made Easy

Cloud-Based Compliance Tools are Critical to Getting Data Privacy and Regulatory Compliance Jobs Done.

White Paper | September 2023

Executive Summary

Healthcare providers work in a very agile environment. Users increasingly leverage software as a service (SaaS) productivity toolsets to complete daily workloads. Products such as Microsoft 365 and Google Workspace offer users feature-rich environments with a wide array of utilities to make their daily lives easier. These tools provide email, social media, productivity applications, collaboration, and convenient storage mechanisms. These tools also provide the benefit of telehealth visits, questions and answers between patients and health providers, and a simple way to keep track of what has occurred over the last few meetings.

In healthcare, regulatory commitments are part of daily life. The Health Insurance Portability and Accountability Act (HIPAA 1996) is likely the first rule that comes to mind. HIPAA's goal is to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. However, there are a few other regulations that are important, such as HITECH (Health Information Technology for Economic and Clinical Health 2009). HITECH is essentially the enforcement wing of HIPAA. There is also the recent Stark Law to prevent fraud and abuse from self-referrals or paid referrals (basic explanation). There are other laws and principles (such as MARCA, Medical Necessity, and Chain of Custody) that provide important pillars to the medical industry.

What does this have to do with healthcare providers' data? Everything. Each of these regulations and concepts has policies for handling and identifying data. What would be a valid set of tools to help a healthcare organization adhere to these concepts? We need systems that can view an organization's data, understand it, and make automated determinations based on the contents. As an example, if you are a research facility and you have projects around genomics, cancer research, Alzheimer's studies, sleep therapy, and more, how do you find your data once it has gone into the system? What if the cure for cancer is sitting in storage and no one can find it? Enter artificial intelligence and machine learning. This process can help researchers find what is important to them. What about the everyday regulatory work that legal, security, and records management need to provide to regulators? How can we be sure PII, PCI, and unstructured medical data are secured?

This is where data governance/management comes into play. The tools are specific in order to get the job done efficiently the first time. Look for tools that will scan the infrastructure looking for metadata (the information about a file—creation date, modified date, size, etc.) and a tool that can scan files and understand their content. This combination will provide exactly what compliance and governance teams need to truly understand their data. Also, the tool that performs the deep scan should be able to categorize that data based upon preset policies that are important to the organization. From there, we can think about what you want to do with the data once it has been scanned and categorized. Leverage tools that are flexible enough to categorize (and tag) data, and help protect data that needs special treatment (such as diagnosis information, personal metadata, drug names, etc.). Does the data get moved to encrypted storage? Moved to the cloud? The better tool will give you these options.

In a recent meeting of the American Health Law Association in Chicago (November 2022), it was mentioned that legal budgets have skyrocketed in recent years. The average small to medium healthcare facility has a legal budget between $10 million and $100 million. This includes all forms of legal consultation, not just litigation. Furthermore, care providers need to find a set of search and data management tools that can locate the data they need, when they need it, no matter the reason. Multiple content sources need to be captured (not just email). If your group is leveraging M365, then at a minimum you will need to capture email, SharePoint, Teams, and possibly OneDrive. There are other content sources to consider as well, such as Zoom, voice to text-based content, Slack, SMS texting, and video are just a few. The next question becomes how do you manage and search the data?

The answer is not just one tool, but a suite of integrated tools. A surgeon does not go into surgery with just a scalpel and a few sutures. The job takes clamps, heart monitors, and other equipment to get the patient healthy. This is also true of a data compliance officer. To complete this task, you need to understand the data and look for patterns in the data (credit card numbers, bank account information, addresses, and more). One of the concepts for this project is eDiscovery. eDiscovery is the process of seeking and finding relevant information in an electronic format, typically done in response to legal matters and internal investigations. The key to eDiscovery is to have an application that can search all your content with a single search (while maintaining a chain of custody). In most cases, M365 needs to search each Microsoft content source separately, making searches repetitive and time-consuming. If you need data from another source, such as Zoom, M365 cannot assist in locating the necessary data.

Another thought to consider is the proactive collection of data. This would apply to content sources such as email and/or Microsoft Teams. Leveraging tools that proactively collect this data allows you to have a full chain of custody (a way to provide audit reporting about the data you have collected) around your data. Also important is that this data is stored in its native format for easy review. Other content sources you will simply collect as needed (Files, OneDrive, SharePoint, etc.) since time frames are not as critical for this type of data. Many organizations may wish to use M365 Advanced eDiscovery for this task, however many recent examples have shown this tool lacking.

How do healthcare providers easily solve this dilemma? The most common response is with third-party applications that are specifically designed to perform individual tasks. One might search for relevant data, another might help with the presentation of that data, another might be used by human resources for data privacy/compliance requests, while another application would help centralize the data. This approach requires a lot of vendors and is difficult to manage and support. The premium solution would be provided by and supported by a single vendor with a centralized support center.

This leads us to third-party eDiscovery and compliance solutions that are based in the cloud, leveraging a software as a service (SaaS) tools that collect the necessary data, secure that data, index, and provide the necessary search tools for eDiscovery and compliance. These tools are traditionally titled as archiving solutions.

However, they are so much more. Before we discuss the important features of an eDiscovery tool, we need to understand what happens when items have not been completely indexed or are not an item that the index engine is capable of indexing. In the case of the Microsoft 365 suite, these are appropriately referred to as partially indexed items. A content search that you run from the Security & Compliance Center automatically includes partially indexed items in the estimated search results when you run a search (this just puts a flashlight on data that is partially indexed).

Although it varies, according to Microsoft's documentation, most M365 customers have less than one percent of content by volume (total number of files) and less than 12 percent of content by size (size of the files) that is partially indexed. The size of files is most important, as larger files have a higher probability of containing content that can't be completely indexed. Therefore, if your organization has one Petabyte of data to search through, the content-by-size data partially indexed could be as high as 120 Terabytes (or 10 Terabytes of content-by-volume partially indexed). This seems like a large amount of missed data that could cause risk.

Google Workspace provides a feature-rich set of tools for its users, with collaboration, messaging, and ease of use at its core. However, Google Workspace provides a limited toolset for compliance and legal teams to respond to today's demands. When capturing email, journaling is the gold standard that messaging and legal teams have relied upon for receiving immutable versions of the email stream containing data not altered or reviewed by the end user. Journaling is a copy of all correspondence that flows through the message transport. Google Workspace only provides the journaling feature in its Enterprise license, which is a very important concern and is covered in a separate Veritas white paper titled, Why do Healthcare Providers Need a Third-Party Archive?. Other features are missing or are not very scalable eDiscovery tools that meet the needs of medium to large healthcare providers. So, let's discuss what Healthcare Providers really need to meet the heavy demands of the compliance and eDiscovery workloads.

For healthcare providers today, it can be challenging to find the solution that best suits the needs of any company, much less a healthcare organization. As we looked at the current offerings from Microsoft and Google, we saw a disparity in features. One tool is feature-rich but is lacking in a few key areas, and the other tool needs serious help in order to provide healthcare providers the tools they need to survive in today's environment. So, where do we go from here?

Even though compliance and eDiscovery review tools come in two varieties (desktop and cloud-based), all review applications share a common set of core features, with some variations. We have seen this in the Microsoft Compliance Center, where there is a set of tools that allow you to get the job done, to a certain point. But now, let us discuss some details. First, there are the big three:

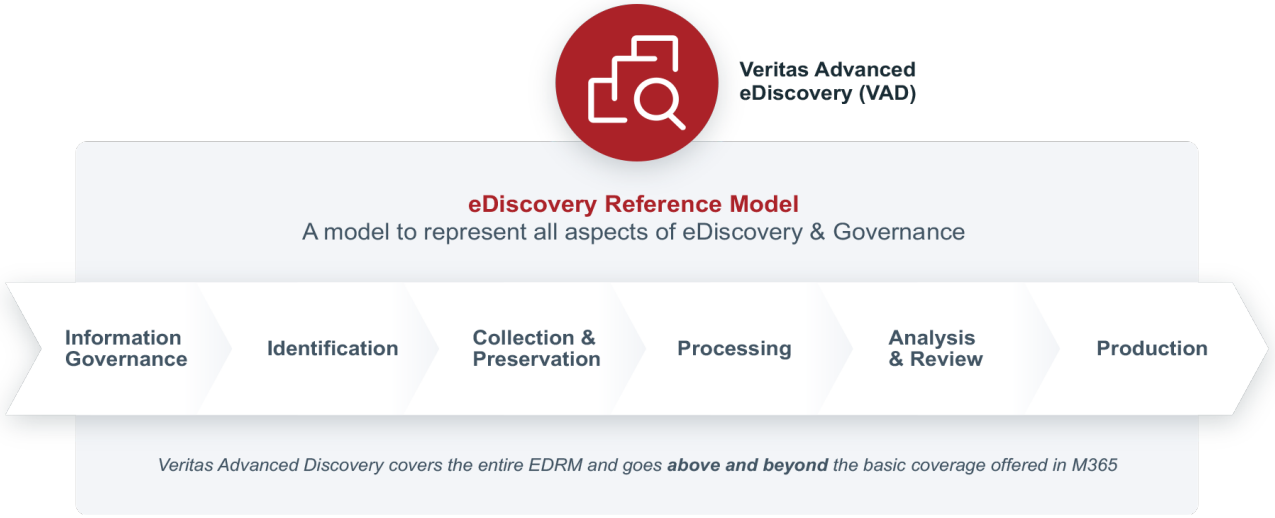
- Recursive Parsing
- Search & Index
- Tagging & Organizing Documents

All enterprise tools have these core features, but let's dive into some extra components that can be extremely valuable. The more features a tool has, the easier the search, review, and presentation of the data.

When looking for a partner to fully comply with legal, compliance, and data privacy needs, there are many features, functions, and benefits to consider. The best way to obtain the best solution for your organization is to be as educated as possible about the technology, and compare the options. Fortunately, a good tool will pay for itself (usually in the first incident) by making document review more efficient, and helping you locate the smoking gun evidence in most cases.

The Bottom Line

At Veritas, we take our customers' governance and compliance needs seriously, and provide a suite of products for these needs. However, no discussion of compliance is ever complete without an understanding of the process of eDiscovery. The Electronic Discovery Reference Model (EDRM) is the foundational workflow that encompasses all necessary steps for successful search and response procedures (please see the diagram below).



Veritas has worked closely with our customers and their investigators/litigators to understand the challenges they face regarding compliance, investigation, and litigation issues. Since many of our customers have faced the same issues, we have incorporated the more common ones into our eDiscovery solution.

The first step is to centralize our data. Traditional archiving tools may have helped in the past, but there are so many ways we touch patients in today's healthcare environment. Our tool is really an ultra-modern data collection solution such as Veritas Alta™ eDiscovery. With the help of Veritas Alta™ Capture (another tool in the Veritas Governance suite of products), Veritas Alta™ Archiving can collect from more than 120 different content sources. This SaaS solution provides a repository for M365 and Google Workspace email and file shares. Veritas Alta Archiving, Veritas Alta eDiscovery, and Veritas Alta™ Surveillance help highly regulated organizations archive data across all communication platforms for seamless migration and automated identification of key content. For compliance officers and corporate legal IT, Veritas Alta Archiving is the proven solution to meet your supervision and discovery requirements.

We discussed earlier that there is a strong need to gather data that is outside of the M365 environment. Content sources such as Zoom, Webex, Twitter, Slack, and others are part of today's environment. To incorporate these content sources into your compliance routine, Veritas offers Veritas Alta Capture. This tool captures high-risk content that is increasingly scattered across dozens of new communication platforms, which makes archiving time-consuming and costly. Veritas Alta Capture captures all business-related data using your existing infrastructure and quickly identifies compliance risks.

We also need a toolset that scans and classifies loose files in the healthcare providers' environment. This is where Data Insight comes in. Data Insight leverages easy-to-use reporting to eliminate waste, reduce costs, and consistently apply data classification policies. Optimize compliance with regulatory archiving from Veritas Alta Archiving; identify data you should keep versus data you can defensibly delete; minimize duplicate, stale, orphaned, and dark data; and enable content owners to easily apply policies through a self-service portal.

The last part of the solution to all these challenges is Veritas Alta eDiscovery, which offers customers the ability to collect from various content sources through a single user interface. Veritas customers are presented with a choice of either having the IT department perform the collections; or allowing the legal compliance or investigation team to do their own collections, completely bypassing IT. This removes the burden of all these collections from the IT department, leaving them to continue their normal jobs and leave the collection to the investigation team. This process gives the investigation team full control over where and from whom to collect data, where to send the collected data, and how the process is managed. The collections module identifies custodians (the subject of the search); has a desktop/laptop search; a collection tool that builds an interactive map of custodians and their data sources; collects to a preservation store (legal hold); and filters data by keyword and metadata. This module provides a single interface to collect from various sources, and reports on what was collected and when, thereby allowing the organization to collect data in a defensible manner.

The next phase is the processing of the data. During this step, the processing and analysis module enables rapid and accurate filtering, processing (indexing), searching, and data analysis in multiple formats and languages. Let us think about indexing. Earlier we discussed the number of items indexed in Exchange Online and Google Workspace, which is only a handful of document types. Veritas eDiscovery Platform can index hundreds of document types, and performs OCR on images, processes audio and video files for search, and categorizes data through multiple policies, making for an easier search. Using the eDiscovery Platform Processing and Analysis Module, corporations, government agencies, and law firms can perform early case assessments, and are able to rapidly cull data. This culling process reduces the overall electronic discovery cost. As an integrated part of eDiscovery Platform, the Processing and Analysis Module also supports the iterative workflows required during real-world electronic discovery. This solution delivers deep insight into case facts and enables a new level of transparency and defensibility throughout the electronic discovery process.

Closing

Unlike the M365 Compliance Center and Google Workspace tools, Veritas (a longtime Microsoft partner) provides a wide variety of tools that stand out in the industry. Veritas Alta (with Veritas Alta eDiscovery, eDiscovery Platform, and Data Insight) provides simple user interfaces with remarkable tools that make the process of data governance, ease of collection, and eDiscovery easy. Whether you are looking for the smoking gun to prove your case, or fulfilling a compliance request, Veritas is the best choice for organizations, legal teams, and compliance officers.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1822 09/23