How to protect digital healthcare assets that are constantly moving and transforming

How to protect digital healthcare assets that are constantly moving and transforming.

Achieve healthcare information protection, while instilling data governance, and ensuring availability on premise and in the cloud.

For more information, contact Carahsoft or our reseller partners:
Veritas@carahsoft.com | (888)-662-2724

How to protect digital healthcare assets that are constantly moving and transforming.

Achieve healthcare information protection, while instilling data governance, and ensuring availability on premise and in the cloud.

VERITAS™

The truth in information.

VERITAS™ WHITE PAPER | MAY 2018

1 THE GROWING DATA DELUGE

The healthcare industry is undergoing a significant digital transformation that is redefining how care is delivered. Whether it's moving from fee-based to quality care or addressing regional health concerns with population health data, healthcare organizations are using the power of information to improve patient outcomes.

It's easy to get lost in the data deluge—which is growing more than 50% per year across healthcare organizations worldwide. New technologies like home medical devices, IoT, and even Fitbits, create mountains of data. According to IDC research, unstructured data accounts for 80% of healthcare information. Furthermore, new clinical protocols leverage as much as 60% unstructured data.

While digital transformation has affected every industry, its impact on healthcare is truly unique given the highly sensitive and critical nature of personal medical information. Protecting that information was not that complicated when all medical records were found in physical files. However, healthcare providers must now protect digital assets that are constantly moving and transforming. They must be able to access medical data within moments to properly handle emergency situations, while also protecting data from unauthorized use. Providers must also be able to share information with each other, with the patient, and with insurers for reimbursement.

According to IDC research, unstructured data accounts for 80% of healthcare information.

Furthermore, new clinical protocols leverage as much as 60% unstructured data.

As healthcare providers face these challenges in an era of unprecedented data scale and of growing unstructured data, they must transform how they manage information to comply with industry requirements and improve patient care.

1.1 ADAPTING TO INDUSTRY TRENDS AND CHALLENGES

HIPAA and EMR requirements: The Health Insurance and Portability and Accountability Act's (HIPAA) most critical requirement is that protected health information (PHI) is secured constantly and in all forms. Violating HIPAA requirements can quickly lead to millions of dollars in fines. Violations defined under HIPAA's Omnibus Final Rule as "willful neglect," in which an organization knows that its PHI is unprotected and chooses not to take action, yields penalties of up to $50,000 per violation with a maximum of $1.5 million per year. In addition, electronic medical record (EMR) providers may impose additional requirements or penalties.

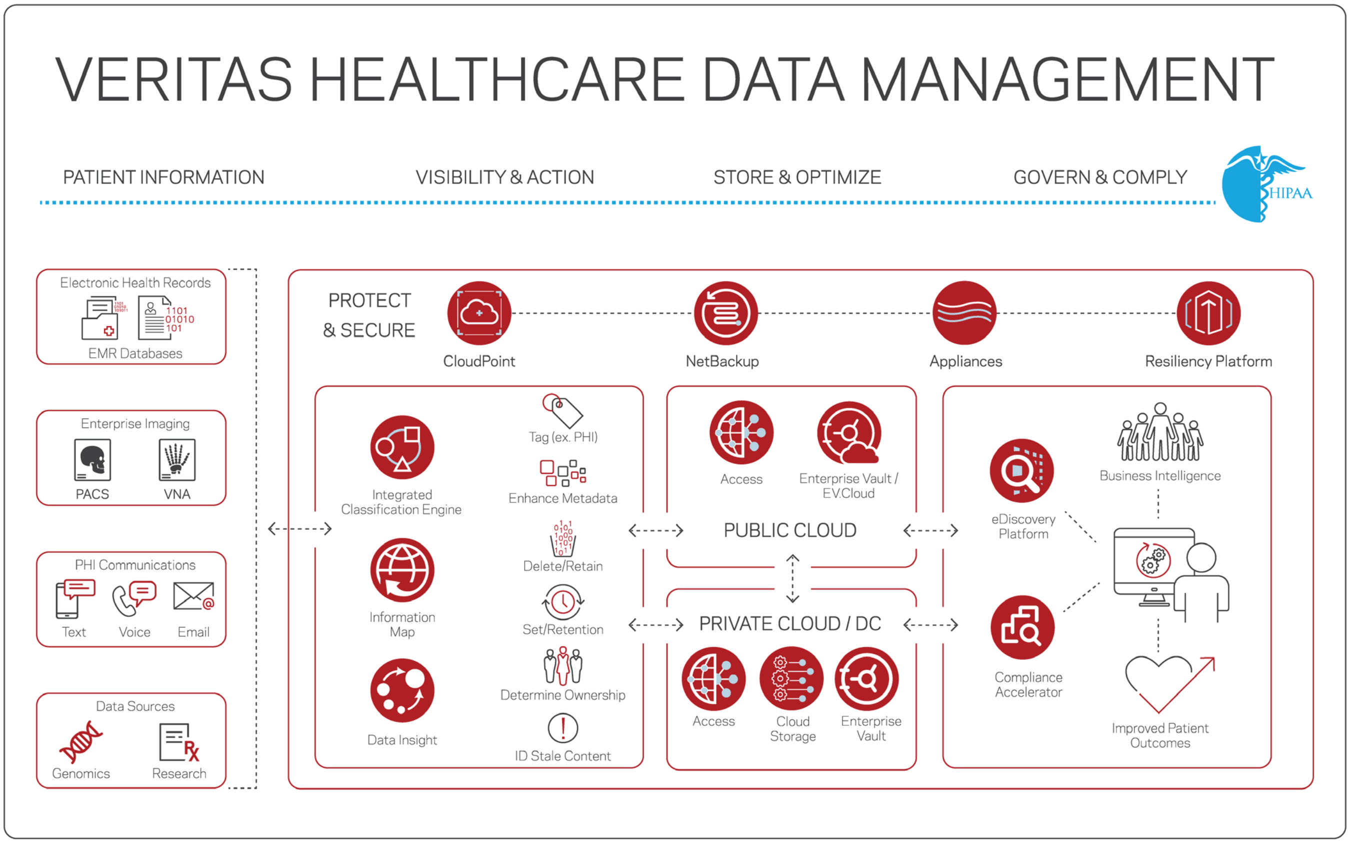
Meaningful Use/MACRA: Meaningful Use measures, and now the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA), are transitioning the entire industry from the idea of "pay for services" to "pay for outcomes." MACRA creates an incentive system for providers in the form of Medicare/Medicaid reimbursements to drive improved outcomes. While MACRA presents a real opportunity for providers, it also comes with the challenge of how to improve outcomes efficiently.

Population health: While all industries face data growth, healthcare is subject to EMR and HIPAA data retention requirements that drive organizations to save data forever. Federal law typically requires data to be contained within the "official medical record" for 21 years, but some state laws require much longer retention periods. With this growing mound of data, it is critical that organizations can extract valuable insights out of their data to help offset retention costs and to improve patient care. Insights, such as the relative efficacy of different treatments or predictive models for the flu season, can result in better reimbursements, new treatment protocols, and cost savings for providers.

2 VERITAS SOLUTIONS FOR HEALTHCARE

So how do healthcare organizations manage the data deluge to comply with these mandates and improve patient outcomes? It starts with visibility. Knowing where your critical information is located gives you the control to properly protect it.

Veritas provides the visibility, security, and protection of both structured and unstructured patient data to give clinicians a better view of a patient's health over time. The visibility and control of your data are prerequisites to complying with HIPAA, and establishing a repeatable HIPAA compliance framework helps improve patient outcomes while increasing reimbursement. Valuable metadata enables healthcare organizations to take appropriate action on how best to store and recover patient data. Veritas reduces the cost of managing data by moving information to the appropriate storage tier based on retention policies and data importance. The figure below outlines Veritas' healthcare reference architecture.



3 HEALTHCARE DATA PROTECTION

For decades, federal law[1] has dictated that organizations keep a backup copy of all protected health information (PHI). Copying PHI to tape and storing it safely offsite was traditionally a viable solution and somewhat addressed concerns of compliance, security, and availability. However, evolving laws, patient care needs, mobility requirements, and technology constraints have made this solution no longer tenable to ensure optimal patient care. Organizations now are finding that PHI legacy solutions are complex, costly, and slow.

A more modern approach to clinical system data protection should result in ensuring and demonstrating compliance, securely protecting patient data in all forms, and ensuring clinical data is available when needed.

3.1 DEMONSTRATING COMPLIANCE

HIPAA mandates that organizations have procedures to create and maintain retrievable exact copies of electronic PHI.[2] Veritas has served the healthcare industry for decades and is fully equipped to support any healthcare organization's data protection and compliance needs.

Veritas NetBackup and **NetBackup Appliances** boast a recovery rate five to seven times faster than the competition—providing you with rapid recovery when you need it most. With a copy of your data in NetBackup, Veritas provides intelligence into the data itself and can orchestrate a full recovery to any platform, premise, or cloud provider. NetBackup can protect your workloads on premise, between premises, and even to—or from—the cloud provider of your choice. NetBackup is certified to protect most electronic medical record (EMR) platforms and many clinical systems, enabling organizations to scale out throughout the entire enterprise.

For example, many large healthcare systems have multiple sites or practices and leverage NetBackup to protect data across the country in a secured data center. This centralizes data protection into an enterprise data center for security and control. Services can then be restored to any region with the click of a button. Other health systems achieve HIPAA's disaster recovery plan requirement[3] by replicating the NetBackup environment to a regionally diverse data center.

Going beyond a simple offsite backup image, **Veritas Resiliency Platform** (VRP) utilizes the backup images to automatically restore services and sequence startups. This solution is crucial to the effective service restoration of complex, multi-tier EMR and clinical applications. In addition, you can have confidence in your disaster recovery plan by routinely testing recovery effectiveness without actually interrupting services via "fire drill" testing. This protects against configuration drift and avoids disruptive tests.

Organizations can also use **Veritas InfoMap** and **Data Insight** for improved data visibility. Leveraging the metadata captured with NetBackup, Veritas InfoMap gives backup and storage administrators visibility into what they are actually backing up. A high-level dashboard displays data amounts and types across the enterprise and enables administrators to drill down. This helps organizations identify all PHI that must be protected, as well as data that should not be protected or on an organization's infrastructure. Such information also allows organizations to make strategic decisions about whether the

[1] The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191.
[2] HIPAA Security Rule, § 164.308(a)(7). Available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf.
[3] HIPAA Security Rule, § 164.308 (a)(7)(ii)(B)).

PHI identified can be appropriately recovered using backup with acceptable RTO/RPO metrics. Data Insight, meanwhile, goes much further, providing intelligence about all of the unstructured data within the organization, helping identify PHI in unsecure locations, such as user workstations or shares, and ensuring data is always protected.

3.2 PROTECTING DATA IN ALL FORMS

HIPAA dictates that patient data be secured at all times, in all formats.[4] In addition, PHI can only be accessed for appropriate clinical and business purposes. However, clinical systems are complex, often consisting of multiple systems, databases, applications, storage arrays, and data centers—making it difficult to monitor access and protect data.

Live production EMR applications and databases are often protected by the access restrictions and endpoint security residing on the hosts. However, these protections are seldom applied to PHI outside of clinical systems. By providing intelligence gathered from backup metadata and unstructured data via Data Insight, Veritas assists organizations in identifying and protecting PHI outside of the EMR. Operational backup and restore is also the safety net for clinical systems impacted by ransomware. However, protecting that data doesn't often extend to the secondary and tertiary storage upon which the data resides, meaning that "defense in depth" is crucial.

Veritas' offerings provide confidence that you can recover data even in the worst-case scenario. The Appliance family hosts the NetBackup software and is deployed with a hardened operating system. Processes running on the appliances are restricted to tasks specific to backup and recovery, while intrusion detection tracks what is being done on the appliances and prohibits unauthorized attempts to access data. Finally, encrypting backups of PHI protects both the patient and the organization from exposure. NetBackup and NetBackup Appliances provide AES 256-bit encryption to protect both data at rest and in motion for backup.

3.3 MAKING CLINICAL DATA AVAILABLE WHEN NEEDED

Data backup, while essential, is only the minimal level of availability. Consider the patient risk if critical data such as blood type, allergies, or medications were not available, or imagine the impact to revenue stream and patient flow if an organization had to wait 48 to 72 hours to recover the EMR. These problems are only exacerbated within healthcare systems supporting multiple regions across the United States.

Demand for patient care systems has never been higher. Reported metrics for Meaningful Use demand continuous availability. Patients also have a right to access their data. Impacted trauma centers or hospitals have a fiduciary responsibility to make relevant PHI available to surviving institutions. Finally, the federal government categorizes healthcare as critical infrastructure, meaning providers must be available during domestic disasters. Organizations that are unable to keep clinical systems available may face class-action suits, OCR investigations, and even loss of Joint Commission accreditation.

Veritas helps organizations define and predictably achieve the proper level of availability for critical technology as dictated by HIPAA.[5] Veritas InfoScale is an approved high availability solution for both EPIC and Cerner. InfoScale will failover

[4] HIPAA Security Rule, § 164.312(a)(2)(iv). Available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf.

[5] HIPAA Disaster Recovery Rule, §164.308(a)(7). Available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf.

automatically to alternative compute, storage, and even facilities or cloud providers. In addition, InfoScale is application aware and can alert or self-heal based on application hangs or lag. It provides service-level availability reporting across heterogeneous hardware, software, and platforms. Critical systems can be configured to failover into the cloud if the on-premise system fails—providing smaller or regional hospitals the means to achieve the disaster recovery requirement if they do not have an alternative data center.

Recognizing that there is no "one size fits all" approach to disaster recovery, Veritas offers organizations a full range of RTO/RPO offerings, from simple tape-based backup for non-critical workloads to always-on mission-critical systems. Emerging "hot" departmental systems that are currently protected with NetBackup can be promoted to the highly available InfoScale with a few keystrokes. Workloads can also be moved to the cloud or between clouds with ease. Veritas' portfolio allows healthcare organizations to manage their workloads and disaster recovery from a single pane of glass.

4 HEALTHCARE DATA GOVERNANCE

In addition to protecting health information and ensuring availability, providers must know what information they have and how to use that data effectively and securely—they need data governance.

A data governance strategy should extend beyond the data contained in the electronic medical record (EMR), as over 80% of the world's healthcare data is unstructured. This includes all electronic communication and all of the organization's files, whether they are stored on premise or in the cloud. While managing all these data sources comes with challenges, it also results in:

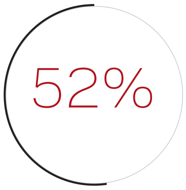
- A complete understanding of your data estate—risks, assets, and vulnerabilities
- Compliance with HIPAA and other relevant regulations
- Enhanced value of content to ease end-user access, discovery, search, and supervision
- New sources of business intelligence and analytics insights

The ultimate goal should be to reach a steady state where content is efficiently stored for as long as it is needed, classified and categorized in near real-time, and ultimately disposed of when/if possible to reduce risk and storage costs. While data governance is required to meet healthcare regulations and to ensure litigation readiness, proper governance leads to cost savings, a more effective workforce, and greater efficiencies throughout the organization.

4.1 UNDERSTANDING YOUR DIGITAL ASSETS

The Veritas Global Databerg Report[6] estimates that 52% of an organization's data is "dark data," which refers to data of undetermined business value. Dark data may hide significant value or compliance risks and may hide valuable content from end users. Healthcare firms, which tend to grow through acquisition, are especially at risk of dark data due to their ever-expanding data set.

Dark Data Assessments should be part of the standard operating procedure when acquiring a new company. File Analysis tools can quickly



According to the Veritas Global Databerg Report, 52 percent of an organization's data is "dark data," which refers to data of undetermined business value.

[6] Veritas Technologies LLC, "Global Databerg Report." https://www.veritas.com/product/information-governance/global-databerg.

determine context around the file, such as ownership and relative value based on prior access. Once a basic understanding is achieved, classification can uncover details that will drive workflow, retention decisions, access controls, and more. Classification can also highlight risks such as personally identifiable information (PII), protected health information (PHI), and credit card data.

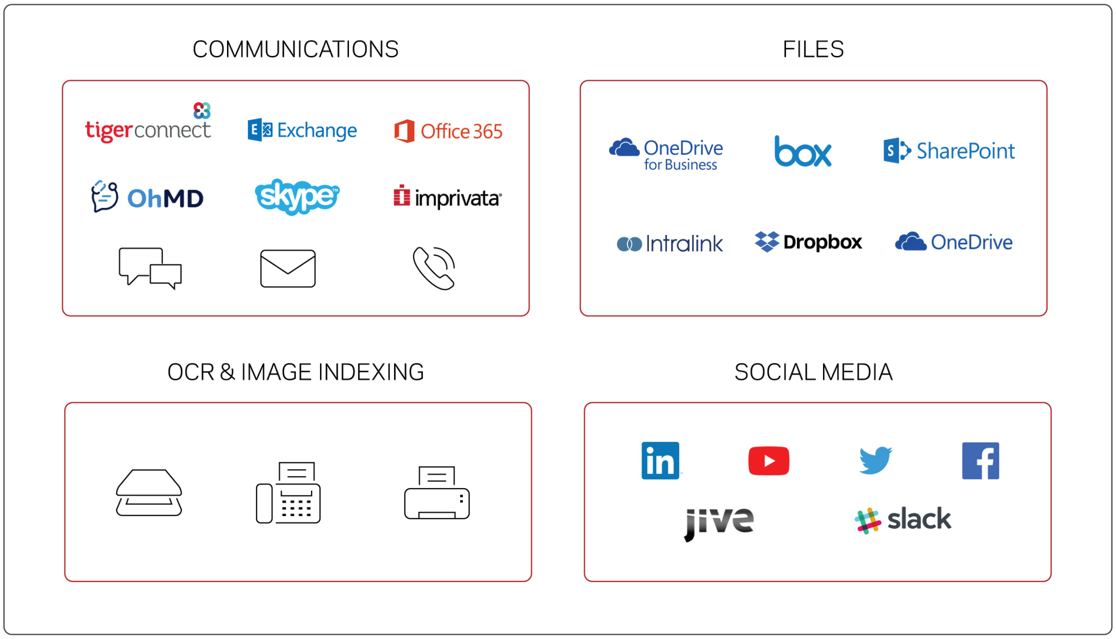
Veritas provides multiple solutions to eliminate dark data. Data Insight drives understanding of both context and content through monitoring, log analysis, and deep classification. Information Map delivers expansive visibility across different cloud and legacy on-premise data stores leveraging metadata from NetBackup and connectors into IaaS, SaaS, and cloud email and productivity solutions. Comprehensive visualization of more than 100 million items can be achieved in as little as 24 hours.

4.2 ENSURING COMPLIANCE

Ensuring compliance from a data governance standpoint requires understanding all the forms of communications and file repositories that are in use within an organization.

Any transmission of PHI must adhere to HIPAA security standards, including:

- PHI is only made available to authorized users who require the information to serve the patient,
- Use of PHI must be monitored when accessed by authorized users,
- Authorized users must authenticate with a unique username and PIN that are centrally issued,
- Policies and procedures to prevent destruction or alteration of PHI, and
- Data being sent beyond the organization’s boundary must be encrypted to make it unusable if intercepted in transit.



The most difficult task is uncovering all forms of communication in a rapidly expanding universe of social and communication tools. Mobile phones, social media, and SMS text are all potential risks for HIPAA non-compliance by medical staff.[7] Veritas' archiving solution, Enterprise Vault, includes a supervision tool called Compliance Accelerator, which can leverage classification to drive review of any communication containing patient or medical information. In addition, providing a viable alternative to text communication, such as a HIPAA-compliant, encrypted texting option, will help ensure adherence to HIPAA without limiting necessary communication or users' personal privacy.

4.3 MAXIMIZING THE VALUE OF DATA ASSETS

According to an IDC research paper first published in 2001, an enterprise with 1,000 knowledge workers wastes $48,000 per week, or nearly $2.5 million per year, due to an inability to locate and retrieve information.[8] Therefore, empowering healthcare knowledge workers to quickly locate the data they need to do their jobs will have a direct impact on patient care, outcomes, and efficiency.

Primarily, federal healthcare organizations may face Freedom of Information Act (FOIA) requests, while all healthcare organizations are subject to litigation and eDiscovery requests. Determining ownership of data, key topics, and classification can make the discovery process more efficient by limiting collections only to relevant data. Classification tags further refine the data corpus prior to producing and redacting the content for release.

Metadata enrichment can also drive business intelligence use cases. Specifically, communications data is an untapped resource for data analytics. Through metadata enrichment (sentiment, key topic/categorization) and existing metadata, organizations can extract valuable information, such as:

- Communication patterns correlated to patient outcomes
- Evidence of communication breakdowns, delays, and net impact
- Response time and frequency of communications between specialists
- Information on subject-matter experts and their areas of expertise to assist with consultation
- Trends in medical staff communications to identify burnout or warning signs, and trends in medical call center communications to identify best practices and problem areas
- Identification of silos and areas to improve communications among geographically dispersed locations

Communication analytics also blends with data points from other systems to further enhance insights and improve patient outcomes.

5 DRIVE DATA TRANSFORMATION

Veritas solutions help healthcare organizations take patient information—from PHI communications, EMRs, imaging, and more—and ensure protection, governance, and high availability on premises and in the cloud. With a multifaceted approach, Veritas helps organizations improve information visibility, optimize storage, apply information governance, and meet compliance requirements wherever their data needs lie. Once they have a handle on their information, healthcare providers can use data more effectively to improve patient care and outcomes.

[7] HIPAA Journal, "Is Texting in Violation of HIPAA?" https://www.hipaajournal.com/texting-violation-hipaa/.

[8] Feldman, S., and Sherman, C., "The High Cost of Not Finding Information." IDC. Available at http://www.ejitime.com/materials/IDC%20on%20The%20High%20Cost%20Of%20Not%20Finding%20Information.pdf.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at www.veritas.com or follow us on Twitter at @veritastechllc.

Veritas Technologies LLC
500 East Middlefield Road
Mountain View, CA 94043 USA
+1 (866) 837 4827
veritas.com

For specific country offices and contact numbers, please visit our website.
veritas.com/about/contact

VERITAS™

The truth in information.

Thank you for downloading this Veritas Whitepaper! Carahsoft is the public sector distributor for Veritas solutions available via the **GSA Schedule 70** contract vehicle.

To learn how to take the next step toward acquiring Veritas's solutions, please check out the following resources and information:

For additional resources:
carah.io/VeritasResources

For upcoming events:
carah.io/VeritasEvents

For Veritas solutions:
carah.io/VeritasSolutions

For Veritas NetBackup solutions:
carah.io/VeritasNetBackup

To set up a meeting:
Veritas@carahsoft.com
(888)-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/VeritasContracts