

Executive Brief

Data sharing vs. data security: Not an 'either-or' proposition

Data sharing is commonly cited as a key to success under value-based care models, which rely heavily on the collaborative efforts of a variety of care providers to improve clinical outcomes.

As a result, healthcare organizations frequently pass imaging data back and forth on CDs, online or through electronic health records (EHRs). In addition, organizations are now sharing data on mobile devices, making it possible for clinicians to access images outside of medical facilities.

But while this data sharing is altruistic and time- and energy-saving in intent, it does have a daunting flipside. Namely, the more data is shared, the more susceptible it becomes to a variety of threats — from cybercrime to employee theft to simple carelessness that results in legal violations.

Feeling the sting of a data breach

When data breaches occur, the fallout can be devastating. Department of Health and Human Services' penalties for HIPAA violations can range from \$100 to \$50,000 per violation, with a maximum penalty of \$1.5 million per year for violations of an identical provision.¹ Organizations can also be subject to expensive litigation emanating from security breaches, not to mention the negative impact such incidents are likely to have on a healthcare organization's overall reputation.

HIPAA violations can result in substantial fines, ranging from \$100 to \$50,000 per violation, with a maximum penalty of \$1.5 million per year.¹

The challenge for healthcare organizations is a tricky one as they seek to provide clinicians with easy access to needed images and data, while also reducing the risk of security breaches — a risk exacerbated by the way in which medical images are stored. Many hospitals currently store and access imaging data through various workstations and multiple PACS. With no overarching storage archive, there are several possible points of failure, introducing the potential for security problems.

Securing data in a VNA 'vault'

A vendor neutral archive (VNA), combined with a universal viewer, can not only provide access to any image, anywhere, any time, but also stores and manage images in a single location. Because a VNA keeps all information in one centralized data repository, organizations can reduce the number of entry points into their systems, making it easier to manage and protect healthcare data.

Some VNAs also provide an extra layer of protection by encrypting archived data. This feature is a welcome addition for IT professionals who recognize the multiple benefits of streamlining systems. After all, with just one system to manage, IT staff are then free to focus on providing greater protection of sensitive information through antivirus software, firewalls and other solutions.

Reducing vulnerabilities by limiting access

A single storage system also means fewer clinicians have access, and as a result, there's a lower likelihood of these storage systems becoming compromised. In addition, VNAs can protect data even further by providing role-based access. This safeguard ensures that only specific individuals view the content they need to perform their jobs.

Perhaps the greatest advantage, though, is that a VNA offers these security advantages without limiting access to the images and data that clinicians and care teams need. In the struggle between data sharing and data security, the right VNA can make everyone a winner.

To learn about Watson Health's award winning VNA solution, IBM iConnect® Enterprise Archive, visit ibm.com/watson-health/imaging

About Watson Health Imaging

Watson Health Imaging, a segment of IBM Watson Health, is a leading provider of innovative artificial intelligence, enterprise imaging and interoperability solutions that seek to advance healthcare. Its Merge branded enterprise imaging solutions facilitate the management, sharing and storage of billions of patient medical images.

With solutions that have been used by providers for more than 25 years, Watson Health Imaging is helping to reduce costs, improve efficiencies and enhance the quality of healthcare worldwide.

Footnotes:

1. HIPAA Violations and Enforcement. American Medical Association. [Accessed January 2018.](#)

© Copyright IBM Watson Health 2020

IBM Watson Health

75 Binney Street, Cambridge, MA 02142

Produced in the United States of America

February 2018

IBM, the IBM logo and ibm.com are trademarks of IBM Corporation in the United States, other countries or both. Merge and its respective logo are trademarks of Merge in the United States, other countries or both. All other company or product names are registered trademarks or trademarks of their respective companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The information in this document is provided "as is" without any warranty, express or implied, including without any warranties of merchantability, fitness for a particular purpose and any warranty or condition of non-infringement. IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with all applicable laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, product or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party

ECM-15829 Rev 4.0