WHITE PAPER

Managing the Growing Demand for Medical Images: Balancing Security and Access

Smartphones and other mobile devices are becoming just as common in the hands of clinicians as they are in the hands of today's teenagers. "Dermatologists, emergency room physicians, ophthalmologists, plastic surgeons and other physicians routinely utilize smart devices to document clinical disorders and pathologies. We have breast surgeons performing ultrasound, neurology doing vascular ultrasounds, urology is performing bladder scans and hospitalists are running around with ultrasound devices for line placements. All this imaging is being performed across healthcare organizations," said Dawn Cram, IT application systems development director for enterprise imaging at University of Miami Health System (UHealth).

Indeed, clinicians are now using smartphones and an array of other mobile technologies to collect medical images. Many clinicians – especially younger care providers – now expect to have access to all kinds of data on their smartphones or other devices.

At the same time, the use of traditional imaging modalities is spreading far beyond the auspices of radiology and cardiology departments. Increased use of imaging promises to improve patient care. However, the rush to fully leverage imaging brings peril – in the form of additional security risks – as well. The problem: The traditional departmental silos of a hospital or health system have created a proliferation of content that has been neglected by enterprise IT organizations. As such, imaging data containing personal health information can be found in stacks of CDs/DVDs, hardcopy

Produced in partnership with

HIMSS Media

> *"When it comes to imaging, security issues stretch far beyond the radiology and cardiology departments."*

Dawn Cram
IT Application Systems Development Director for Enterprise Imaging
University of Miami Health System

photos in file cabinets, isolated desktop computers, USB drives and smartphones. So, while the picture archiving and communication systems (PACS) used in radiology and cardiology departments offer reliable image management and security functionality, the disorganized and dispersed image capture, storage and access methods now being deployed by other clinicians and departments across the enterprise are creating the potential for increased security risks and compliance violations.

"Because there's a plethora of imaging that is now being conducted outside of radiology and cardiology, healthcare CIOs, CEOs and other executives need to understand with this vast growth in image capture and methods comes additional security risks," Cram said. "Healthcare leaders cannot simply ignore these risks or hope that they will go away. They have to realize that when it comes to imaging, security issues stretch far beyond the radiology and cardiology departments."

Facing the new reality

As organizations continue to leverage imaging in greater numbers, leaders need to be aware of two critical issues:

The unique security risks associated with mobile devices. Smartphones are becoming a standard part of many physicians' workflow because they now offer high-quality images, can handle a variety of image-capturing tasks when equipped with advanced lenses and can perform a broad array of functions by leveraging a growing number of clinical apps.

As with any technology, however, there are security risks, according to Lee Kim, JD, CISSP, CIPP/US, director of privacy and security at HIMSS. "Mobile technology is nascent. Mobile devices can be easily lost, stolen, or the wireless communications may be eavesdropped," she said.

Because of this vulnerability, healthcare organizations should take a comprehensive approach when addressing data security on these devices, according to John Hansen, vice president of interoperability solutions at Merge Healthcare. To do so, it's important to get answers to a variety of questions such as: Do clinical images taken with a smartphone get uploaded or transferred to the cloud? If so, does the cloud have proper security safeguards? If the image is stored on the phone, is the phone password protected or easily deciphered? Can unauthorized users look at the images or steal the phone? Is there a business associate agreement in place that covers the security of data accessed through a smartphone app?

The move to value-based care. As healthcare organizations zero in on improving quality and outcomes under value-based models, the need to acquire and share images across the continuum of care is expected to escalate. As a result, organizations will need to balance the demand to access images with the need to protect them.

"My prediction is that there will be a significant increase in point-of-care imaging over the next 10 years as we move into value-based care (VBC). With the rapid advancement of handheld image capture devices and movement toward patient-centric [care], organizations will be expected to provide imaging as part of the patient visit," Cram said. "As we move to a VBC [value-based care] model, it will become increasingly important that we're also looking at security in the context of appropriate accessibility. Flexibility has to be addressed and understood with an approach and strategy developed."

> *"The challenge rests in giving care providers access to as much patient data and imaging as possible in a secure fashion."*

John Hansen
Vice President, Interoperability Solutions
Merge Healthcare

Achieving balance

While healthcare leaders need to be aware of all potential security risks associated with medical-imaging proliferation, they understand that imaging supports quality patient care. As such, they need to deliver both greater access to and enhanced protection of imaging data.

"Healthcare organizations want this imaging proliferation to happen because it is so vital to patient care," Hansen said. "The challenge rests in giving care providers access to as much patient data and imaging as possible in a secure fashion."

What's needed is a comprehensive enterprise data management program that will provide clinicians with much-needed access to images, while simultaneously protecting data in a secure manner that complies with patient privacy regulations such as HIPAA. "Care providers need to have the same at-their-fingertips, role-based access to medical images as they have to electronic health records data," said Hansen. "But controls also need to be in place to protect the images from being seen by unauthorized staff."

A strong enterprise data management strategy can mitigate the security and compliance risks found in many self-managed specialty departments, while offering the access to images clinicians need. The first step in implementing such a program is to "stop the bleeding" by purchasing image-capturing devices that have the ability to store images in a centralized location. After purchasing appropriate devices, organizations need to implement an enterprise imaging management program that includes storing images centrally; ensuring security and compliance with IT oversight to centralized data; and adding appropriate accessibility and workflow to improve patient care.

Deploying vendor neutral archive and enterprise viewer

An enterprise-wide image data management strategy with a vendor neutral archive (VNA) at its core helps organizations better access, manage and protect the plethora of images emanating from diverse image-capturing modalities. A VNA combined with an enterprise viewer not only provides access to any image, anywhere, any time, but also safely stores and manages images in a centralized location. Such a system can archive all images, Digital Imaging and Communications in Medicine (DICOM) and non-DICOM.

UHealth, for example, is making it possible to use a wide variety of image-capturing modalities by leveraging Merge Healthcare's iConnect® Enterprise Archive, a VNA capable of storing and managing an array of image types.

In addition, the health system has deployed an app that makes it possible, through a greatly improved workflow process, to directly send files from image-capturing devices to the VNA. With these solutions in place, clinicians can capture images with a variety of devices – and the information associated with the image is then validated and sent to the VNA using Cross-enterprise Document Sharing for Imaging (XDS) profiles. As a result, the enterprise archive serves as both the DICOM repository and an XDS repository.

> *"With VNAs, clinicians have access to the same images in a centralized location."*

Lee Kim, JD, CISSP, CIPP/US
Director of Privacy and Security
HIMSS

With the VNA-supported enterprise data management strategy in place, UHealth is "now able to pull or ingest any standard file that can be dropped on the network, determine if the imaging follows an encounters-based or orders-based workflow, validate the images against the appropriate EHR record and then send the content to the VNA using an XDS profile," Cram said.

As such, UHealth is now able to accommodate a broad range of imaging preferences. For example, the enterprise imaging management initiative is able to handle a variety of "service lines like dermatology and surgery, [even though] their typical imaging workflow does not align with the traditional approach," Cram said. Instead of forcing healthcare professionals to struggle with manual steps and multiple proprietary systems, the Merge system at UHealth is now capable of ingesting 90 percent of enterprise imaging content including JPGs, PDFs, video and audio.

This encounter-based imaging process uses XDS profiles, which also enables "physicians [to] take a photo, and based upon the body part localization that they do on the smart device or camera, wirelessly send that photo to the archive and automatically associate it to the patient visit in the EHR," Cram said.

With VNAs, organizations can easily manage access to images with the appropriate levels of security relevant to the user's role in the organization and in compliance with regulatory requirements. "Leaders only have to worry about one centralized storage area as opposed to having images on laptops, CDs, USB drives, smartphones," Kim said. "With VNAs, clinicians have access to the same images in a centralized location."

Because VNAs typically make it possible to provide role-based access to the images, leaders can ensure that clinicians only see what they are authorized to see. Some VNAs can even provide the ability to "break the glass" and allow users to gain access to locked-down images as needed. In these situations, the VNA immediately documents who has seen what and the justification for doing so – ensuring HIPAA compliance.

When organizations leverage VNAs as part of an enterprise-wide strategy, they can fully embrace imaging in all its forms, while also addressing inherent security risks. "With an enterprise data management strategy, organizations are making it possible to provide the access to imaging that is needed to succeed in this era of value-based care and, at the same time, the security control to ensure patient privacy and security in this era of mobile technology," Cram said.

Produced by HIMSS Media | www.himssmedia.com | © 2016

ECM-12171 Rev 1