

Sponsored by

Canon



HEALTHCARE INFORMATION EXCHANGE: TRANSFORMATION DURING CRISIS

By BPO Media for Canon

Canon U.S.A. does not provide legal counsel or regulatory compliance consultancy, including without limitation, Sarbanes-Oxley, HIPAA, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality/performance; you may want to test these settings in your environment.

HEALTHCARE INFORMATION EXCHANGE: TRANSFORMATION DURING CRISIS

Abstract

The COVID-19 pandemic has put increased pressure on healthcare information management systems, with effective healthcare information exchanges required to help acquire, manage, exchange, analyze, and protect healthcare data. Key challenges remain in interoperability, accessibility of information for patients and caregivers, and the security of the information and the various IT systems used to store, manage and share it. This paper reviews these three challenge areas and covers what a healthcare organization can consider when choosing and working with a technology vendor in building a strong and transformative digital healthcare information exchange system.

Author

Tom O'Neill

Senior Analyst, BPO Research

Published by BPO Media

About BPO Media

BPO Media is a publishing, marketing, and research firm. Its BPO Research division provides market research and consulting services focused on office technology, workflow, process optimization, and the transformation resulting from the ongoing integration of digital and mobile technologies. BPO Media's other divisions include BPO Marketing and the Office Technology Group, which produces the leading trade publications The Imaging Channel and Workflow. Visit www.workflowotg.com, www.theimagingchannel.com, or email info@bpomedia.com.

Contents

- HEALTHCARE INFORMATION EXCHANGE: TRANSFORMATION DURING CRISIS 1
 - Abstract 1
 - Author 1
 - About BPO Media 1
- Healthcare Information Exchange: Transformation During Crisis 3
 - Meeting Old and New Challenges in Healthcare Information Management 3
 - Overcoming EHR Interoperability Challenges to Strive for Successful Patient Outcomes 3
 - Accessibility of Patient Healthcare Information 5
 - Information Security 6
 - Summary 10
 - Learn more about the solutions mentioned in this article: 10
 - References..... 11

Healthcare Information Exchange: Transformation During Crisis

Meeting Old and New Challenges in Healthcare Information Management

The COVID-19 pandemic introduced the most significant threat to worldwide health since the 1918 Spanish Flu outbreak and put new impetus on the ability to quickly gather, share, analyze, and act on healthcare data. Organizations that had focused on effective health information management since the Health Information Technology for Economic and Clinical Health ([HITECH Act of 2009](#)) was put in place to promote the adoption and meaningful use of health information technology were already familiar with these needs. Healthcare providers have been focused on digitally transforming their information management processes to help improve the accuracy and efficiency of healthcare information exchange which could ultimately help with healthcare service delivery across the continuum of care a patient receives.

Improving the quality of patient care to achieve successful health outcomes is the primary objective of any healthcare professional. Meeting that objective requires effective healthcare information exchange, and that calls for the acquisition, management, sharing, analysis, and systems that can help protect the patient's healthcare information. Electronic healthcare records (EHR) are a foundational part of healthcare information exchanges. They contain clinical and non-clinical patient information that caregivers need to provide diagnoses, treatment, and ongoing care for their patients. Spread across various systems and functions, this information can be difficult to consolidate into a centralized EHR system. Key challenges remain in interoperability, accessibility of information for patients and caregivers, and security of the information to not only comply with regulations such as HIPAA but also to help protect the various IT systems used to store, manage and share it.

This paper will review these three challenge areas and what a healthcare organization should consider when choosing and working with a technology vendor in building a strong and transformative digital healthcare information exchange system.

Overcoming EHR Interoperability Challenges to Strive for Successful Patient Outcomes

Government mandates and financial incentives due to the HITECH Act have fueled the use of EHRs in the last 10 years. Hospitals and other healthcare providers invested in EHR systems that met meaningful use requirements to receive more than [\\$30 billion in incentives paid by Medicare](#) through 2018ⁱ. Despite this increased adoption, though, there can still be some interoperability challenges that can hinder the effectiveness of EHRs.

A patient's EHR is created from information found in millions of data points scattered across various systems. Sources of this data can include paper records converted to digital form, computerized healthcare records, diagnostic imaging devices, medical monitoring equipment, patient wearables, emails, and admitting and billing systems. Together, they build a valuable single-source record of a patient's diagnoses, treatment, and complete medical history. Using a single digital record allows healthcare professionals across the continuum of care to help deliver optimal outcomes in quality of care with speed, accuracy, and privacy compliance.

Effective EHR communications are inexorably linked to successful patient outcomes. In a [recent study](#), 69.9% of participants said the ability to communicate effectively with colleagues electronically was a successful outcome of using EHR, while 48.2% of participants cited the opportunity to share results with patients as another successful outcome.ⁱⁱ Good EHR systems are key to telehealth services, which ranked No. 2 in top-of-

mind priorities of healthcare IT professionals in 2019. As the COVID-19 pandemic unfolded in 2020, [telehealth innovation jumped to the No. 1 spot for 2021](#).ⁱⁱⁱ

However, despite the successes EHR systems can provide, there are still challenges that can be addressed to help improve the ease of use and reduce friction between healthcare information exchange systems. Interoperability between the systems and processes that contain patient information can be critical to ensure an EHR is complete, up-to-date, and accurate. Unfortunately, a lack of interoperability between these systems and processes can cause headaches for IT administrators, could lead to clinician burnout, and potentially impact the quality of care to the patient.

In the most recent report to Congress, the Office of the National Coordinator for Health Information Technology^{iv} reported that 90% of non-federal acute care hospitals were electronically sending or receiving (exchanging) patient health information with healthcare providers outside their organization. While that is good news, the report also revealed:

- Less than two-thirds (61%) could electronically find patient health information from sources outside their health system.
- Only 53% could integrate (without manual entry) health information received electronically into their health IT system.
- Almost half (49%) did not have access to necessary patient health information electronically available from healthcare providers or sources outside their systems at the point of care

A primary recommendation from that report is to improve interoperability so healthcare providers can more easily exchange and analyze patient information. The COVID-19 pandemic has made that recommendation even more important.

What are the tech issues affecting healthcare IT? A [HIMMS/Forrester survey](#)^v asked a group of healthcare IT professionals, “What is the most pressing technology issue you are facing now that you need the vendor community to prioritize?” Perhaps not surprisingly, the top two answers related to meeting the challenge of interoperability between healthcare information systems:

1. Integrating new solutions like virtual care and remote collaboration with existing clinical workflows.
2. Sharing data across an increasingly fractured continuum of care, including patients.

Meeting these challenges will not be easy, as most EHR systems have proprietary architectures, but the message is clear: Technology vendors must prioritize interoperability between healthcare data systems, content management systems, clinical analysis, business process systems, and all other systems that work together to create EHRs.



2018 ONCHIT Report to Congress

Top recommendation

“Focus on improving interoperability and upgrading technical capabilities of health it, so patients can securely access, aggregate, and move their health information through their smartphones (or other devices) and healthcare providers can easily send, receive, and analyze patient data.”

[*Annual Update on the Adoption of a Nationwide System for the Electronic Use and Exchange of Health Information*](#)

CANON SOLUTIONS WITH INTEROPERABILITY IN MIND

CONTENT MANAGEMENT

- Therefore
- mxHero

PRINT MANAGEMENT

- uniFLOW
- uniFLOW Online

It is difficult to find one technology vendor with the answer for all interoperability challenges. However, just as healthcare specialists and professional support teams work together in a hospital to provide whole healthcare coverage, healthcare providers should seek technology providers that do the same. Look for providers that are best in their practice of content management, process management, and data analytics, and who have a deep understanding of requirements and standards such as DICOM, IHE, HL7, and FHIR for interoperability.

Paper and printing continue to be a large part of healthcare information management, so print management must also be part of the equation to help create a seamless and secure data flow between ongoing paper-based systems and digital systems. Vendors should be able to demonstrate that their products, solutions, and services can seamlessly integrate with other systems and healthcare processes in use, and work across a variety of data

formats. The result for the healthcare provider can be a holistic EHR strategy with strong interoperability that can deliver communications and reporting between colleagues, peers, the patient, and entities outside of the primary provider that can result in cost-effective outcomes and improved patient satisfaction.

Accessibility of Patient Healthcare Information

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) codified a patient's legal right to access their healthcare information. When HIPAA was enacted, however, most health records systems were paper based, so searching for, copying, preparing for delivery and mailing personal healthcare information to meet patient requests was time-consuming, cumbersome, and expensive for healthcare providers. The increase in use of EHRs and advancements in digital information delivery platforms has made it more efficient for healthcare providers to provide patients timely access to their own health information, and for the provider to more efficiently and securely share it with other caregivers. These advancements have also allowed for more efficient healthcare information exchanges between healthcare professionals as they seek to gain a more complete picture of a patient in their care.

Patients are taking a more active role in managing their health.

[Sharing clinical results with patients](#) was reported as a benefit in using EHR systems by [48.2%](#) of healthcare providers.^{vi} Digital devices and mobile apps are used to manage their health by [64% of patients](#)^{vii}, and [93% of patients](#)^{viii} are able to view their health records online.

Using devices such as laptops, tablets, smartphones, and electronic wearables, healthcare information can now be accessed from virtually anywhere at any time. Patients can review their information at home or on the road. Caregivers can view, analyze, and share a patient's information from their office, while traveling, in hospital emergency and operating rooms, or while visiting and caring for patients in private long-term healthcare facilities or hospice.

93% of patients can view their health records online.

[American Hospital Association](#)

“With COVID-19, things were upended. Within just over a week, we went from no telehealth to 2,000 telehealth visits per day.”

Healthcare CMIO, “COVID-19 Pandemic Shifts Innovation Priorities at Health Systems.”

Though not all health organizations have been using telehealth or telemedicine practices, these practices have been on the healthcare innovation horizon for some time. COVID-19 fueled an exponential need to implement these practices as it became apparent virtual healthcare services were essential to mitigating the spread of the disease.

One [healthcare CMIO](#) said, “With COVID-19, things were upended. Within just over a week, we went from no telehealth to 2,000 telehealth visits per day.”^{ix} Improving the ease of access to health information for both the patient and the healthcare provider helps health organizations deliver effective virtual healthcare for traditional needs while also giving them the ability to directly service COVID-19 patients. Telehealth and the need to support easy access to health information contained in EHRs will continue to grow, even after the threat from COVID-19 has subsided.

While responding to COVID-19, the healthcare industry was not spared the need to follow local stay-at-home directives for employees. Though many frontline nurses and doctors were called upon to meet COVID-19 head-on in their work with hospitalized patients, there were also clinicians, diagnosticians, and support staff that were asked to work from home. With technology solutions that allowed them access to EHRs and other digital information, they were able to collaborate with colleagues, conduct their usual workflows and deliver normal healthcare services to patients while supporting the fight against COVID-19. Even before the COVID-19 threat, [75.5% of healthcare professionals](#) said having access to this information was a success factor in EHR systems.

Accessibility to healthcare information is impacted by the interoperability issues outlined in the previous section. Information access sites such as patient portals need to support the variety of data that make up a patient’s EHR. This includes text documents, spreadsheets, emails, PDF, DICOM images, and multiple video, audio, image and other file formats. Systems also need to support chat, teleconferencing, and videoconferencing. Of course, this functionality needs to be available and properly formatted for use across all platforms a patient or other caregiver might use to access this information, including PCs, laptops, smartphones, and tablets. Healthcare providers accessing health information need all of the above as well as systems that use [artificial intelligence](#) (AI) to transform information into “smart data” that can be used to provide improved diagnoses and treatment services.

When selecting a technology vendor for content management, process automation, or information processing, the vendor’s ability to integrate with healthcare information exchange access systems is an essential consideration. The solution proposed should be able to support the various viewing platforms a patient or caregiver may use. This provides convenient access and viewing of health information as a health organization pursues a holistic healthcare information exchange strategy.



CANON SOLUTIONS
SUPPORT ACCESSIBILITY

- Therefore
- mxHero
- Box

Information Security

In a pre-COVID-19 [national survey](#) done by the American Medical Association, 83% of physicians reported experiencing some form of cyberattack and 74% of them were concerned that a cyberattack would not only interrupt business practices but also compromise EHR security. In a sobering statistic, 53% expressed concerns that a cyberattack could pose a real threat to patient safety.^x As the COVID-19 threat materialized in 2020, USA

Today reported that “between March and April, IBM saw a [6,000% increase in spam attacks](#) on information technology systems, leveraging COVID-19, many of them at healthcare facilities .”^{xi}

In the healthcare industry, the cost of a data breach resulting from a cyberattack or as the direct result of something like a ransomware attack can potentially be high in dollars and human life:

- Compared to other industries, the healthcare industry has the [most expensive data breaches](#) worldwide, with the costs of those breaches reaching more than \$7 million annually.^{xii}
- A healthcare data breach costs, on average, [\\$408 per record stolen](#) - three times higher than the average of all other industries, globally.^{xiii}
- In 2020, the first [patient death attributed to a cyberattack](#) was reported as a critically ill patient died while in transport after being diverted to a different hospital after the initially intended hospital suffered a ransomware attack.^{xiv}

The ease with which EHR and digital healthcare information exchange allow patients and healthcare organizations to have access to private health information, and to share and act upon that information, has also introduced potential data breach points and vulnerabilities that can be left open by unwitting patients, employees of health organizations, and others. These can be exploited by malicious actors to obtain sensitive confidential information or carry out IT system cyberattacks. Sadly, only 46% of organizations say they are effective in preventing cyberattacks.^{xv} However, there are some simple measures a health organization can take to secure their EHR and healthcare information exchanges to attempt to minimize and mitigate some cybersecurity risks.

1. Leverage security capabilities in the content management, process management, and data analytics software solutions that are part of a healthcare information exchange system. Organizations can look for systems that allow them to enable features that can help with the following:
 - Capture information early and often and drive it to a secure repository that is regularly backed up – whether on-premise or in the cloud.
 - Encrypt both data at rest in servers or cloud repositories, and data in motion over the internet to the intended users using strong encryption key strategies.
 - Set permissions for users authorized to access, edit, and share information.
 - Use multifactor authentication (MFA) in addition to strong PIN and password methods to verify any user attempting to sign on to the system.
 - Add metadata that provides un-editable audit logs or audit trails that can be used to show who accessed, edited, and shared the information, how often this was done, when it happened, and with whom the information was shared.
2. Implement security in every critical step in the creation and distribution of information, including printers and multifunctional devices (MFDs) that continue to be used to print, scan, and fax billions of clinical pages every year as paper-based processes continue to be part of healthcare information exchanges. It is important that printers and MFDs have security features enabled that monitor and control access to help ensure the device is not used as an entry or endpoint for a cyberattack.



CANON imageRUNNER ADVANCE MFP SECURITY

- Verify System at Startup
- McAfee Embedded Control
- SIEM Integration
- Authentication with function level log-in

These features include those such as are included in many Canon MFPs:

- Secure system startup with a secure boot protocol that tests to see if malicious code has infected the device and, if it has, that the device does not boot up on the network.
 - Built-in, ongoing virus and malware protection.
 - SIEM integration.
 - Trusted Platform Module (TPM).
 - Hard disk drive encryption, overwrite, and erasure.
 - Print encryption/decryption.
 - Role-based access to the device and all its functions, controlled by authentication using PIN, password, or proximity card methods.
 - Secure print to ensure only the print job sender with the correct PIN, password, or authentication method can release their print job.
3. Control and manage the output produced by printers and MFDs with print and scan management solutions. Whether these solutions are implemented using on-premise or cloud-based servers, they should be able to:
- Encrypt print data from PC/laptop/mobile device to the printer or MFD and, particularly for a cloud print management service, encrypt print data in transit.
 - Enable role-based access and authentication to the device and all its functions via PIN, password, proximity card, or other methods.
 - Provide secure pull printing so only the authenticated user can access their print jobs and select which job to print, rather than printing all jobs in the queue.
 - Provide an audit trail of what was printed, when it was printed, and who printed the document.
 - Have a form of keyword intercept that will halt a print or scan job and notify IT or other key organization members if someone is attempting to print or scan a document containing sensitive words or terms identified by the organization.
4. Implement an intelligent email management system. Email is an often-overlooked part of healthcare information exchange security as attachments containing sensitive patient information can be sent with no way to control who views, copies, or forwards the information. Phishing attacks can obtain sensitive information from unwitting email recipients or deliver malicious code as file attachments that an unsuspecting employee downloads. Ponemon lists phishing as the top security threat identified by organizations, with the average cost of a phishing attack at \$832,500.^{xvi} COVID-19 brought an increase in the number of phishing attacks as work-from-home employees in healthcare were outside the strong email security protocols of corporate networks. Intelligent email management solutions can offer a layer of email security to help both remote and on-site workers with patient information security.

CANON INTELLIGENT EMAIL MANAGEMENT SOLUTIONS

- [Box](#)
- [mxHero](#)
- [imageRUNNER ADVANCE MFPs](#)

Select intelligent email management solutions can establish rules on who can receive file attachments, how long they have to download the file, and whether the recipient can forward the file. Also, they can remove attachments on incoming emails, saving them to a secure cloud content storage solution, replacing the attachments in the email with links to the stored file. Employees preview the file in a web browser to determine if it is recognizable before opening it on their computer. This can help mitigate the possibility of downloading a malicious file. Intelligent email management solutions can automate

these processes and make the secure archiving and classification of emails as well as attachments seamless and invisible to the employee. They should:

- Seamlessly integrate with email clients and cloud content storage solutions to store both the email itself and any attached files an email contains, as well as incorporate content access permission controls.
- Feature intelligent and automatic filing of the email and attachment files to designated folders of the content storage solution based on the To, From, Subject, and other context in the email.
- Provide manual and automatic metadata tagging to facilitate the governance, e-discovery, or retention rules of the cloud content storage system, which can lead to faster and more accurate searches across emails and attachments.
- Provide audit trails of who received file attachments and warnings if an attempt to forward the attachment is made.
- Ideally, be a cloud-based SaaS model with no need to download software onto employees' computers.

Of course, enabling technology security features in software, email, or print devices does not guarantee the elimination of all data breaches or possibilities of cyberattacks. However, it can help with the security of network endpoints, which 35% of organizations identified to Ponemon as [security vulnerabilities](#).^{xvii} Unfortunately, the leading cause of security vulnerabilities is [negligent insiders](#), as reported by 40% by organizations.^{xviii} This means that it is imperative to continue security training, software training, and device training so that employees understand the seriousness of cybersecurity and know how to use the security technologies and protocols the health organization puts in place.

Not only do patients expect sensitive medical information to be kept private, accurate, and secure, HIPAA states this as one of a patient's rights. Health organizations must have security mechanisms and standards in place that not only safeguard this patient information but also protect the organization from cyber threats that may use healthcare information exchange endpoints to attack the larger IT infrastructure. Organizations should look for technology vendors that can demonstrate their content management, process management, data analytics, and print solutions deliver security features that an organization can implement to help it protect healthcare information and IT infrastructure.





Summary

The healthcare industry's digital transformation in healthcare information exchange is fully underway. Although the increased use of EHRs may have initially been driven by the financial incentives surrounding meaningful use, the benefits of improved access to information are now being widely embraced by the health community. The efficiency of the growing use of telehealth and telemedicine relies on having a single source of record of a patient's health history, diagnoses, and other pertinent medical information accessible to the healthcare professional wherever they may be and on whatever device they use to review that information. With the digitization of data systems, information and network security has extended from just ensuring patient privacy rights to an organization safeguarding the complete healthcare information exchange system from cyberattacks. The COVID-19 crisis has accelerated this transformation in healthcare information exchange throughout all these areas and its impact will be felt well into the future.

As hospitals and other health organizations navigate through the current COVID-19 crisis and beyond, the selection of technology vendors in support of healthcare information exchange and the use of EHR is more important than ever. They should seek vendors that understand the interoperability, information accessibility, and security challenges faced and who have innovative solutions to these challenges. Vendors with software solutions complying with standards and that have nonproprietary APIs allow more nimbleness integrating with other vendor solutions an organization uses. Since paper processes are still a part of the healthcare information exchange, considering a printer or MFD vendor that has integration with software solutions used in an EHR system and that delivers device and output security is a must. Considering and selecting vendors that meet these requirements can put a healthcare organization on track to creating a holistic, and efficient digitally transformed healthcare information exchange.

Learn more about the solutions mentioned in this article:

<https://www.usa.canon.com/internet/portal/us/home/explore/industries/healthcare/>

Print Management	Content Management	Intelligent Email	Security
uniFLOW	Therefore	mxHero	Canon MFD Security
			

Canon U.S.A. does not provide legal counsel or regulatory compliance consultancy, including without limitation, Sarbanes-Oxley, HIPAA, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality/performance; you may want to test these settings in your environment.

References

- ⁱ Zachary R. Murphy, M. (2020). Association of EHR Use Above Meaningful Use Thresholds With Hospital Quality and Safety Outcomes. <https://bit.ly/35sJgZU>
- ⁱⁱ Philip J. Kroth, M. (2019). Electronic Health Record Design and Use Factors and Clinician Stress and Burnout. <https://bit.ly/2Tjqqus>
- ⁱⁱⁱ Research Report: COVID-19 Pandemic Shifts Innovation Priorities at Health Systems. (2020). <https://bit.ly/3ojtbyk>
- ^{iv} 2018 Report to Congress, Annual Update on the Adoption of a Nationwide System for the Electronic Use and Exchange of Health Information. <https://bit.ly/3mbmwV9>
- ^v HIMSS and Forrester Partner to Understand Technology Motivation. 2020 <https://bit.ly/2TpQXdI>
- ^{vi} Philip J. Kroth, M. (2019). Electronic Health Record Design and Use Factors and Clinician Stress and Burnout. <https://bit.ly/2Tjqqus>
- ^{vii} Survey: Patients Regard Open Access to Their Medical Records as Critical to Receiving High Quality Health Care, Business Wire. 2017. bwnews.pr/3msjko7.
- ^{viii} Sharing Data, Saving Lives. (2019). Retrieved from <https://bit.ly/35xTF6W>
- ^{ix} Research Report: COVID-19 Pandemic Shifts Innovation Priorities at Health Systems. (2020). <https://bit.ly/3ojtbyk>
- ^x Medical cybersecurity: A patient safety issue. (2018) <https://bit.ly/2HvbR8H>
- ^{xi} USA Today. (2020). A game of 'cat and mouse': Hacking attacks on hospitals for patient data increase during coronavirus pandemic. <https://bit.ly/3ksqKau>
- ^{xii} Cost of a Data Breach Report 2020. (2020). <https://ibm.co/34neZMQ>
- ^{xiii} Cost of a Data Breach Report 2020. (2020). <https://ibm.co/34neZMQ>
- ^{xiv} ZDNet; First death reported following a ransomware attack on a German hospital. (2020) <https://zd.net/2J1zYwA>
- ^{xv} The Economic Value of Prevention in the Cybersecurity Lifecycle. (2020) <https://bit.ly/3olXZhR>
- ^{xvi} The Economic Value of Prevention in the Cybersecurity Lifecycle. (2020) <https://bit.ly/3olXZhR>
- ^{xvii} The Economic Value of Prevention in the Cybersecurity Lifecycle. (2020) <https://bit.ly/3olXZhR>
- ^{xviii} The Economic Value of Prevention in the Cybersecurity Lifecycle. (2020) <https://bit.ly/3olXZhR>