

A stronger healthcare system in the age of COVID: Strategies for robust patient data sharing, **cybersecurity** and **interoperability**

To create a stronger healthcare system, we need secure technology that enables the frictionless transfer of data across hospitals, health systems and the world. Now is the time for radical innovation. This final guide in a four-part series shows what's working in healthcare today and what's possible to build for our future needs.



Introduction

This is a crucial opportunity for innovation

At this critical moment for our nation's health systems – at a time when a global pandemic is incentivizing hospitals to **extend care** beyond their walls and **optimize workflows to improve the quality** of care – seamless interoperability underpinned by cybersecurity is essential to successful patient care. By ensuring that technologies work together across platforms and geographic locations, we better protect the data that flows **throughout our health systems**. And when data is secure, we're able to confidently extend care to reach veterans, American Indians, Alaska Natives and many more no matter where they receive treatment – whether that treatment is delivered across multiple touchpoints within an enterprise, in community centers and retail locations across the country or even inside patients' homes.

The cost of inaction is high

These are not new imperatives, but COVID-19 has made them even more urgent. Health systems were already facing substantial difficulties in exchanging data at the micro- and macro-level: from devices to departments, from department to department, from hospital to hospital and even into patient homes. Those challenges have manifested in an inability to track longitudinal patient data and exchange information across different vendors. That miscommunication alone can cost the US healthcare system \$1.7 billion per year,¹ and the disorganization across systems creates vulnerabilities as well. In 2019 alone, 510 healthcare data breaches were reported – a 196% increase from 2018 – exposing 41.3 million patient records.² Those breaches, which in the past decade have affected up to 90% of health systems, have an average cost of \$3.86 million each.^{3,4}

When data doesn't flow across technologies, care suffers

These vulnerabilities and miscommunications contribute to operational and clinical dilemmas

as well. For example, 80% of serious medical errors involve miscommunication between healthcare providers during the transfer of patients.⁵ When information is not readily available and actionable, patient care can be impacted – for example, patients can end up staying in ICUs longer than necessary, which results in overcrowding, delays in care, exposure to errors, financial consequences and even psychological problems, such as posttraumatic stress disorder (PTSD) and depression.⁶ For many veterans – and potentially for our nation's service members as well as American Indians – depression⁷ and PTSD⁸ are prevalent, which makes it all the more important that we minimize unnecessarily lengthy ICU stays.

These challenges further affect a health system's ability to use the advanced analytics that interoperable data make possible, which limits their ability not only to manage current operations but also to extend care delivery – and protect the systems and information within the growing enterprise.

The future belongs to frictionless and secure care delivery

For all of these reasons, interoperability and cybersecurity are key characteristics of an efficient healthcare system – and they are especially important now given the requirements of the 21st Century Cures Act, which mandates that health systems cannot block the sharing of patient information with patients and providers or incur hefty fines and that individual providers will incur loss of Medicare funding.

Whereas the implementation of closed systems has been prevalent, Philips believes that a stronger healthcare system depends upon **secure, multivendor-positive, well-integrated technology** that provides the advantage of actionable insights and clinical decision support. The good news is that we have the platforms, the processes and the pedigree to do just that.

Two strategies for interoperability and cybersecurity

To close the capacity and capabilities gap, health systems will need to:

Connect data and technology

Leveraging open APIs and approved standards like IHE-HL7 to enable seamless data exchange across multiple sources and vendors throughout the continuum of care so healthcare providers can deliver the right care at the right time in the right place with minimal friction.

Secure data and systems

Taking a proactive approach to protecting sensitive health technology and patient information across devices, systems and settings so administrators, healthcare providers and patients have confidence in how care is delivered.



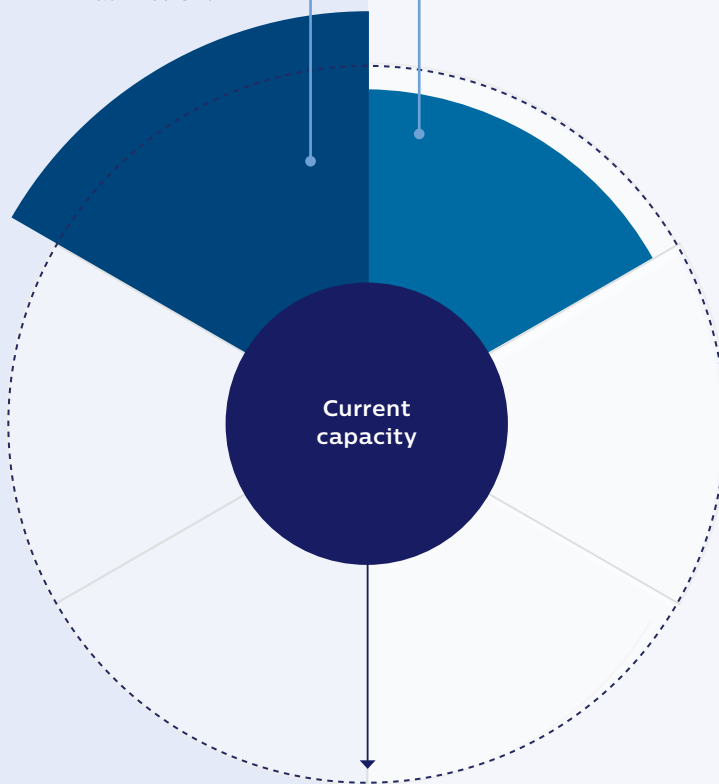
Frictionless connections



Scalable technologies



Multivendor positive



Standards based



Protected patient information



Smooth exchange across points of care

Needed capacity

Taking a platform view

In this guide, we take a platform view of interoperability and cybersecurity, prioritizing the seamless flow of data through secure systems regardless of vendor, and we suggest ways you can transform your health system. Taking a platform approach also allows for nimble innovation that addresses the diverse needs of today and of the future.

To illustrate our position, we take a look at the government's largest health system – the US Department of Veterans Affairs (VA) – plus a geographically distributed clinical network and a nationwide data-sharing portal to demonstrate how Philips is helping data and technologies work together across extended care locations within hospital departments and within enterprises to turn disparate and dispersed data into actionable insights.



Key takeaways



Connecting technologies and data

An interoperable healthcare system is a stronger one where data flows seamlessly across devices and locations.



Providing better care across the continuum

When technologies and data connect, health systems can better care for patients and communicate clearly with patient advocates across every step in the patient journey.



Meeting urgent needs in every community

Better care and communication are especially important during crises when hospitals rely on telehealth and other points of care outside their walls and when care is extended into remote areas.



Empowering healthcare providers

When data flows across technologies, healthcare providers can access the right data at the right place and the right time, improving their clinical decision-making.



Securing systems from attack

Technologies designed to work together are better organized and more secure from malicious online attacks.



Innovating at scale

Philips multivendor-positive, standards- and platform-based approach connects disparate technologies, maintains component flexibility and creates a system of engagement that sets up our customers for long-term growth and better health outcomes.

Connect **data and technology**

Scalable technologies tailored to changing needs

Let's imagine a health system built to be truly interoperable and secure. That health system is one that provides a new digital front door for patients and supports and secures a patient's frictionless journey across healthcare settings, points of care and events. This may begin within a single hospital, where well-defined care pathways rely on seamless transitions between specialized tools and teams. And, as care continues to extend beyond a single hospital to include more locations, more vendors and more cloud-based solutions, interoperability becomes even more critical to make information securely accessible to patients and providers. It's that kind of coordinated care that allows health systems to deliver a holistic, multipronged approach to care throughout the patient journey.

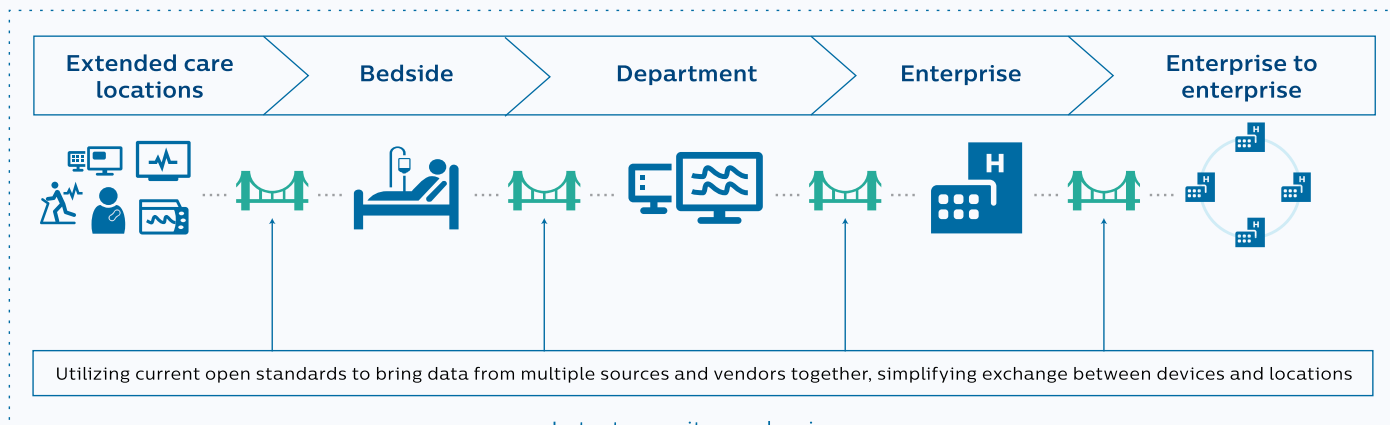
A health system built with a person's care experience in mind supports a widening variety of patient audiences and advocates, too. As the balance of care shifts to prioritize care beyond the hospital – and in many cases, focus on keeping patients out of the hospital entirely – health systems face the need to share data with multiple stakeholders. Sharing data with everyone from patients and healthcare providers to families and

proxies requires accurate identification of the patient, stringent access permissions and granular controls.

These challenges are even greater during pandemics as care delivery shifts to virtual care or telehealth visits. Care delivered in communities, homes, retail and other government environments, like VA healthcare facilities, allows for remote screening and triage and the proactive management of patients in low-acuity and lower-cost settings. In these settings, new types of patient interactions – both synchronous and asynchronous – put a premium on device- and setting-agnostic care. Interoperability also amplifies the impact of data from multiple sources, such as **remote patient monitoring (RPM)** data and **diagnostic medical devices**, allowing a provider or clinician to view patient records and near real-time RPM or device data during visits.

Through our work with customers and our support and leadership of technology standards, Philips strives to help make interoperability and security a core component of health systems across the country. By taking a platform view to help technologies and data work together, we can enable better clinical decision-making and better health outcomes at scale.

Philips interoperability solutions help make **frictionless connections across healthcare**



Philips enterprise platforms

Case study: **Connecting care** for the country's largest health network

As the largest federal health system, the VA provides healthcare to nearly 9 million veterans across 18 regional Veterans Health Integrated Network Administrations, 175 hospitals, more than 1,000 Community Outpatient Centers and several hundred Veterans Centers, Mobile Vet Clinics and Access Telehealth Local Area Stations locations.

Maintaining such a large network comes with challenges. Roughly 5 million veterans live in areas designated as rural by the US Census Bureau,⁹ making access to healthcare difficult. And as that population ages, the prevalence of chronic conditions, like hypertension and diabetes, is projected to rise by 12% and 8%, respectively.¹⁰ Difficulty in accessing care is further exacerbated during pandemics, when patients need to receive certain care from home and when reduced rates of admission for heart attacks, strokes and other emergencies suggest that patients might be avoiding necessary care out of a fear of going to the hospital.¹¹ In 2020 there has been a 56% decline in in-person visits across VA outpatient facilities, which is only partly offset by the twofold increase in the number of telephone and video visits.¹²

Extending secure care across devices and locations

To combat these trends, enhance the experience of veterans, caregivers and survivors, and make healthcare as accessible and affordable as possible, the VA needed a virtual health solution that extended access to care while helping to coordinate team members and putting information sharing and cybersecurity at the strategic center of its clinical technology. That is, the VA needed technologies and data to work together across devices and locations, and they needed the data that flowed between those devices to stay secure.

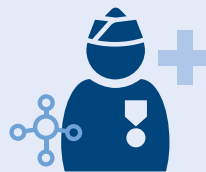
To deliver on that vision of device- and setting-agnostic care, the VA selected Philips to understand their clinical needs, assess the existing level of interoperability, understand documentation requirements and ultimately provide the equipment for **virtual care sites** within Veterans of Foreign Wars and American Legion posts throughout the United States.

Serving those who served our country



18+ million

people cared for by the VA and the DoD's Military Health System,¹³ making these two of the nation's largest and most complex health systems¹⁴



9 million

veterans enrolled in the VA healthcare system, including 3 million living in rural areas¹⁵



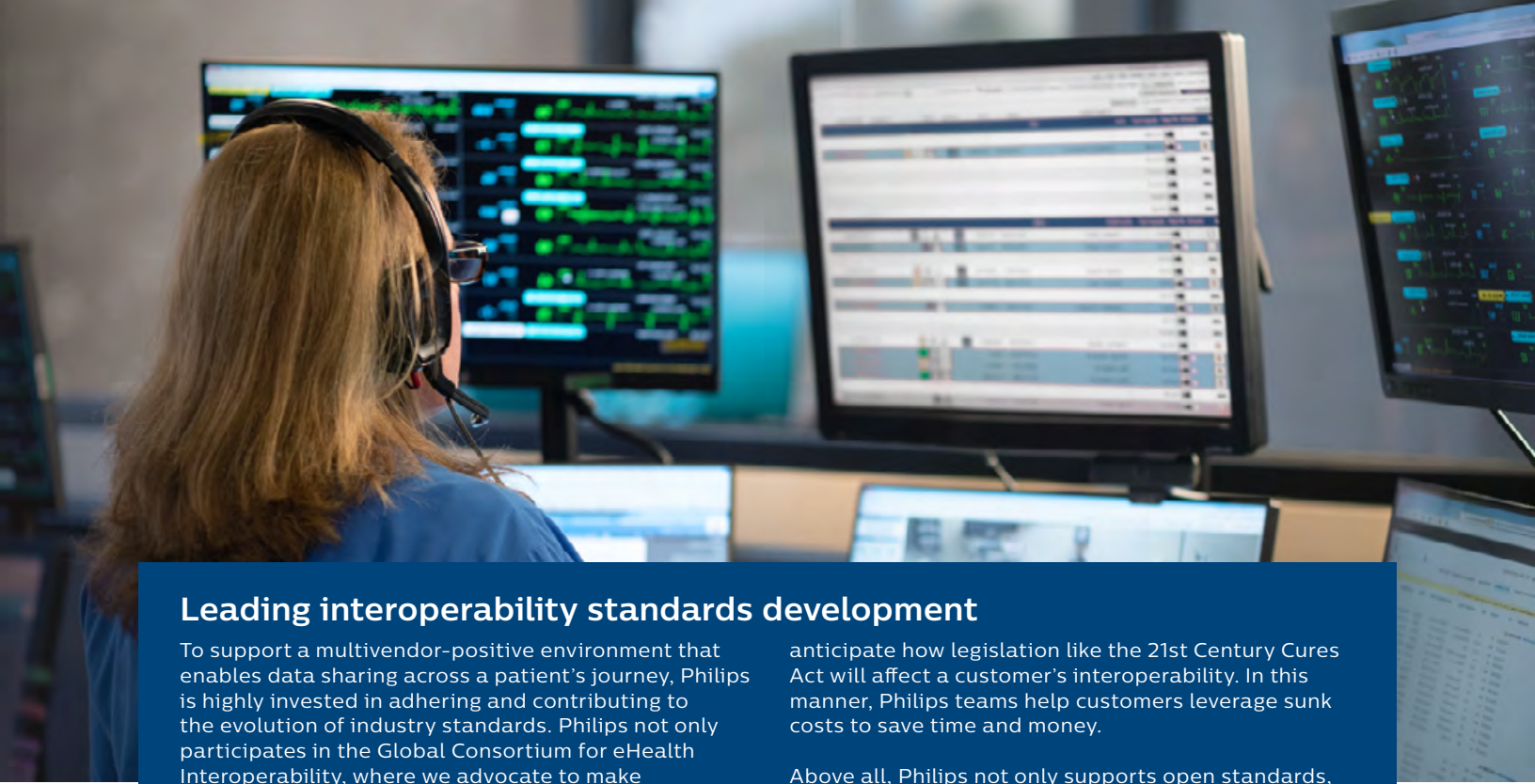
2.5+ million

VA video telehealth visits facilitated in 2019, a record for the VA¹⁶



1000%

increase in VA video telehealth visits during the first weeks of the COVID-19 pandemic¹⁷



Leading interoperability standards development

To support a multivendor-positive environment that enables data sharing across a patient's journey, Philips is highly invested in adhering and contributing to the evolution of industry standards. Philips not only participates in the Global Consortium for eHealth Interoperability, where we advocate to make policy-based interoperability road maps a reality, but we were also an early adopter of HL7's Fast Healthcare Interoperability Resources (FHIR) specification, a standard for organizing and describing healthcare data for ease of exchange between systems. This gives Philips perspective on how the healthcare industry will adopt new standards and allows Philips teams to

anticipate how legislation like the 21st Century Cures Act will affect a customer's interoperability. In this manner, Philips teams help customers leverage sunk costs to save time and money.

Above all, Philips not only supports open standards, but also works toward their implementation, supporting vendors at every level. This allows systems and departments to communicate with each other and exchange clinical information inside and outside the enterprise, helping partners and customers to collaborate and create a truly effective care collaboration ecosystem.

This work, which aims to untether patients from a centralized location, will in part fulfill the mandate of the MISSION Act, which stipulates that veterans can receive healthcare at either a VA facility or another general provider within the community. Such a mandate increases the need for interoperability of EMR and diagnostic imaging data with the Department of Defense (DoD), private health networks and clinicians. Or, in other words, if the patient is free to move, the data needs to be free to move as well.

Keeping patients healthier outside the hospital

This allows care to be delivered in lower-cost and more accessible settings, helping the VA to improve the consistency of care and focus on preventative care to keep patients healthier outside the hospital. In the event patients move between care settings, the VA can ensure that they are better served throughout their journey.

Interoperability makes connecting care possible

An interoperable virtual care system is one where data flows easily and securely across every component. This ability has the potential to improve the clinical decision-making process across the health continuum by giving healthcare providers access to the right data at the right place and the right time. It also allows care workers to reach veterans no matter where they've

decided to live and work and can also facilitate direct access to EMR from points of care. By getting components and data to work together across time and place, this interoperability can ultimately improve veterans' satisfaction with their care.¹⁸

A tightly knit, cohesive virtual care system that makes data sharing easy is also a system that is easier to protect from online attack. To ensure data security, Philips is committed to working closely with the VA through both the Federal Risk and Authorization Management Program (FedRAMP) and the enterprise risk assessment (ERA) process, addressing potential material weakness in network-connected devices by identifying the inherited risk and impact, addressing system-specific security controls and managing and addressing vulnerabilities. And, because of our commitment to interoperability, Philips technology, like **modular and extensible transport monitors**, provides secure clinical decision support throughout the patient journey – from the field to transport to bedside – ensuring uninterrupted care. By doing so, Philips aims to help healthcare providers and patients alike have greater confidence that care will be quickly, conveniently and, above all, securely delivered.

This level of planning positions the VA for the future as well. Veterans qualify for care in part based on their

Integrating systems to increase access to care in rural areas and tribal lands

Like many veterans, American Indians and Alaska Natives face challenges getting access to the healthcare they need. Healthcare needs to be delivered in tribal lands and in rural areas that can be sparsely populated and where citizens potentially face chronic conditions, including heart disease, respiratory issues, and unintentional injuries – the likelihood of which was noted in the recent Executive Order on Improving Rural Health and Telehealth Access, which seeks to improve access to healthcare in rural areas through telehealth technologies.¹⁹ Philips partners to securely deliver the care that is promised to these populations, including virtual technologies like eICUs that enable co-located teams of specially trained critical care physicians and nurses to monitor patients and virtual care sites that allow for the frictionless transfer of EMR, diagnostic imaging and other data while shifting the focus to routine and preventative care.



economic health; public health emergencies, such as COVID-19, have the potential to radically expand eligibility and benefits for millions of veterans. By conceiving of the patient journey as an interoperable virtual care solution, the VA will secure both its patients' health and the integrity of its continuum of care.

Giving veterans access to the right care at the right time

The same technology, patient-centered workflows and clinical approach can also be used to serve veteran patients in their home or at their local veterans service organization. These solutions, including virtual care sites now being **piloted across the country**, will allow veterans to be examined at their local post through virtual appointments with medical professionals across the nation – saving veterans travel time and expenses, reducing admissions for those with health risks and increasing the focus on preventative care. The sites include electronic scales, blood pressure cuffs, thermometers and pulse oximeters.

This kind of consumer-centric model – interoperable and consistent across patient encounters and settings beyond the hospital and clinics with endpoints in the home, the workplace, the retailer and more – provides a more convenient and accessible care experience. With this investment in virtual care, the VA positions itself to focus on preventative care and manage home-based care models with the same rigor as a clinical service line. When care is digital, there is consistent and clear continuity from the hospital to the home.

Importantly, these forms of care will allow the VA to create economies of scale beyond the traditional visit model. With a digitally networked provider organization, supported by data interoperability, analytics and device integration, the VA not only can monitor and manage beds in multiple medical centers across zones but also can manage utilization of care – so that patient access, provider staffing and appropriateness of care can be optimized. Such a system, when enabled with scalable IT infrastructure, can be extended to cover expanding populations across geographies for greater economies of scale.

Moving forward

The VA recently announced that it also plans to **invest up to \$100 million over a 10-year period** with Philips to expand its tele-critical care program, thereby providing veterans access to the right intensivists and quality care, regardless of their location. With the VA managing 1,800 ICU beds nationwide, this expansion not only gives patients access to specialists but also helps them deliver on the quadruple aim: optimizing care costs, enhancing clinician and patient satisfaction and improving outcomes.

Philips continues working to supply state-of-the-art technologies, workflows and approaches, which means the VA can increasingly put veterans at the center of care. Philips is proud to help the VA accomplish that goal safely and effectively via interoperable and secure technology.

Secure data and systems

Health data breaches and malicious online attacks like ransomware are arguably two of the biggest worries keeping healthcare leaders up at night.² As health systems extend more care into patient communities and homes, health systems are transitioning from managing data and technologies on-site to managing data and technologies across an external continuum of care. The complex network opens up opportunities for compromise.²⁰

But a health system where technologies and data work together – where smooth data exchange occurs across points of care – is a system that is easier to secure against malicious online attacks. At Philips, we take a proactive approach to protecting sensitive health technology and patient information across devices, systems and settings so that we can help administrators, healthcare providers and patients have confidence in how care is delivered.

Integrating data for more secure and better-managed care

As health systems expand and merge, the confluence of multiple technologies and processes across practices and locations can hamper an administrator's ability to develop insights on how to manage care. To say it another way: It's hard to understand how to build for the future if each of your building materials uses a different standard of measurement. That was exactly the challenge faced by Eastside Health Network (EHN), a joint venture clinically integrated network (CIN) that needed a cost-effective way to quickly aggregate data across two large health systems in Washington State.

Philips worked with EHN to build a comprehensive view of their patients across 1,352 physicians, 185 practice locations, 40 practice billing systems, 20 EHR feeds and 10 payer feeds. Integrating that information – coming from 90 different data sources – further allowed for the creation of intuitive, easy-to-read dashboards to engage user teams with different reports for different needs, providing the data they need to close care gaps, identify high-risk members and manage care.²¹

Powered by integrated data and actionable insights, EHN was able to quickly progress to more advanced contracts – including shared savings, downside risk and fully capitated programs. What's more, the interoperability of their systems enhanced the security of their networks, so they could confidently grow their business and provide care to 35,000 members and growing. [For more information about Philips work with EHN, see our case study.](#)

Sharing secure COVID-19 data at the touch of a button

The ability to share data among hospitals and authorities becomes an even more acute need during



Interoperable and secure technologies provide the data health systems need to manage care.

a pandemic, when the timely sharing of secure medical records can dramatically affect the use of shared healthcare resources – and potentially save lives.

In cooperation with Erasmus Medical Center (Rotterdam, the Netherlands), Jeroen Bosch Hospital ('s-Hertogenbosch, the Netherlands) and the Netherlands Ministry of Health, Welfare and Sport (VWS), Philips developed an online portal that allows Dutch hospitals to seamlessly share COVID-19 patient information with one another at the touch of a button. Connecting over 95% of Dutch hospitals, the COVID portal allows clinicians to share specific patient data – such as a patient's radiology images, reports and patient summary – assisting in critical activities like the transfer of infected patients between hospitals to avoid local overload in critical care units. What's more,

this data is transferred without links to an individual hospital's electronic patient dossier (EPD) and only transferred if the patient has given their consent, thus ensuring privacy.

By building this portal on top of the hospitals' existing XDS cloud document sharing service, Philips Interoperability Solutions helped to ensure that the portal only increased the system's inherent cybersecurity and maintained compliance with the ISO27001 information security standard and the Dutch NEN7510 standard, which is specifically designed for information handling in the healthcare sector.²²

For more information about Philips work, please see [National Portal for Digital Exchange of COVID-19 Patient Data in the Netherlands](#).



Certified secure care for our country's service members

To provide our government partners with cutting-edge equipment and to ensure that connected devices and systems meet or surpass security standards, Philips is committed to ensuring our technologies meet US government specifications including the DoD's Risk Management Framework (RMF), FedRAMP and the VA's ERA process. By performing to these specifications, Philips can better enable the system-wide availability and cybersecurity of patient data and diagnostic images for clinical staff, thereby facilitating more timely and effective care.

- **HealthSuite System of Engagement certified by HITRUST:** This extensive set of external compliance certifications and attestations provides objective evidence of compliance to security and privacy regulations such as ISO 27001/18, SOC2.
- **Underwriters Laboratories (UL) product cybersecurity testing certification:** Philips is proud to be the first medical device manufacturer to be granted this certification, which combines cybersecurity testing elements of the established UL 2900-2-1 standard for Software Cybersecurity for Network-Connectable Products, as well as security principles from international standards (ISO 13485 and ISO 14971).²³

At Philips, 'security by design' is an end-to-end mindset. Security principles and controls are integrated into all aspects of product development and testing starting with product design and development through testing and deployment and followed with robust policies and procedures for monitoring, effective updates and, where necessary, incident response management.

Summary

We're in a critical moment in our nation's history when the challenges of caring for aging populations and a public health crisis demand that we be even more innovative about technology's use – and more vigilant about its potential misuse.

The opportunity in this moment is to expand our healthcare system's capacity and capabilities in a way that untethers caregiving from physical locations and extends care to where our patients live and work.

There is nothing more critical to this evolution of care – nothing that affects the success of our health systems and the future of patient care more than seamless interoperability underpinned by cybersecurity. Interoperability facilitates the data exchange that ensures the continuum of care is unbroken. Cybersecurity, a key component of interoperability, means data is protected and that administrators,

clinicians and patients can have confidence in how information is managed so care can be effectively delivered.

A health system built to be truly interoperable and secure is a health system that supports and secures a patient's seamless journey across healthcare settings, solutions and events – and it's a health system that can evolve to meet the changing needs of tomorrow.

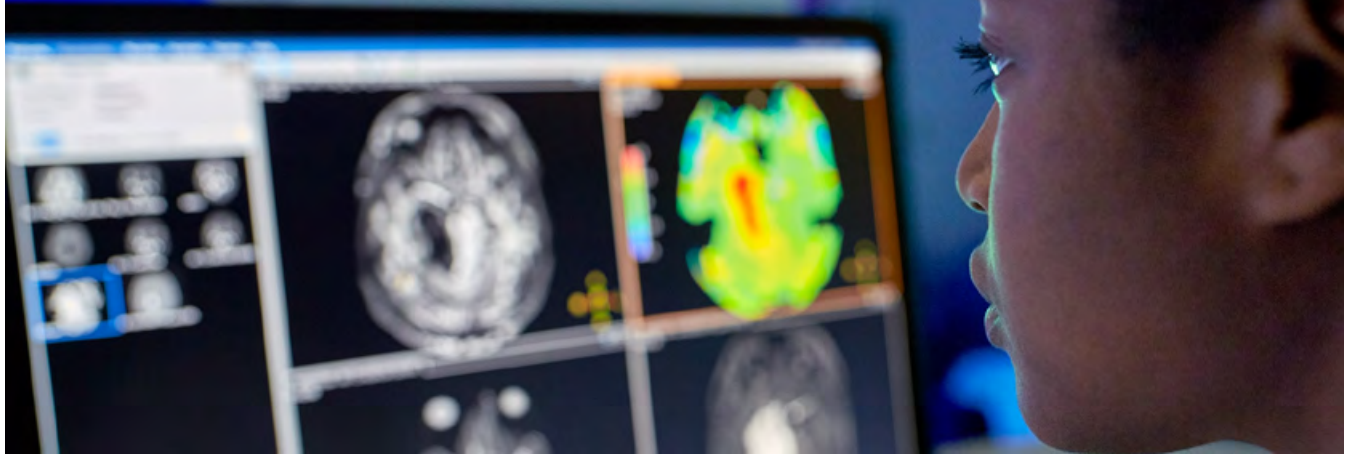
To help build stronger healthcare systems, we're publishing a series of guides that offer strategies, tactics and resources. This is the fourth of four guides. The previous guides include:

- [A path to building a stronger healthcare system for a stronger America](#)
- [Extending where and how care is delivered for a stronger healthcare system](#)
- [Building a stronger healthcare system requires optimizing clinical and operational workflows](#)

Results from case studies mentioned in this paper are not predictive of results in other cases. Results in other cases may vary.



We're in a critical moment when we must be even more innovative about technology's use and vigilant about its potential misuse.



References

1. CRICO Strategies. *Malpractice Risks in Communication Failures*. <https://www.rmhf.harvard.edu/Malpractice-Data/Annual-Benchmark-Reports/Risks-in-Communication-Failures>
2. HIPAA Journal. 2019 healthcare data breach report. Accessed August 25, 2020. <https://www.hipaajournal.com/2019-healthcare-data-breach-report>
3. The Ponemon Institute. *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*; May 2016.
4. <https://www.usa.philips.com/healthcare/articles/cybersecurity>
5. Joint Commission Center for Transforming Healthcare releases targeted solutions for hand-off communications. *Jt Comm Perspect*. 2012;32(8):1-3.
6. Blanc L, Abillama FF, Amin P, et al. Triage decision for ICU admission: report from the Task Force of the World Federation of Societies of Intensive and Critical Care Medicine. *J Crit Care*. 2016;36:301-305.
7. Gould CE, Rideaux T, Spira A, et al. Depression and anxiety symptoms in male veterans and non-veterans: the Health and Retirement Study. *Int J Geriatr Psychiatry*. 2015;30(6):623-630.
8. Gradus JL. Epidemiology of PTSD. US Department of Veterans Affairs. Accessed August 10, 2020. <https://www.ptsd.va.gov/professional/treat/essentials/epidemiology.asp>
9. <https://www.census.gov/content/dam/Census/library/publications/2017/acs/acs-36.pdf>
10. RAND Health. *Current and Projected Characteristics and Unique Health Care Needs of the Patient Population Served by the Department of Veterans Affairs*; 2015.
11. Krumholz HM. Where have all the heart attacks gone? *The New York Times*. April 6, 2020. Accessed June 20, 2020. <https://nyti.ms/2UN1tNN>
12. Baum A, Kaboli PJ, Schwartz MD. Reduced in-person and increased telehealth outpatient visits during the COVID-19 pandemic. *Ann Intern Med*. 2020;M20-3026.
13. Veterans Health Administration. About VHA. Accessed August 10, 2020. <https://www.va.gov/health/aboutvha.asp>
14. Military Health System. Beneficiary population statistics. Accessed August 10, 2020. <https://www.health.mil/I-Am-A/Media/Media-Center/Patient-Population-Statistics>
15. VA Office of Rural Health. Rural veterans. Accessed August 10, 2020. <https://www.ruralhealth.va.gov/aboutus/ruralvets.asp>
16. <https://www.usa.philips.com/a-w/about/news/archive/standard/news/press/2020/20200708-va-selects-philips-to-create-worlds-largest-tele-critical-care-system-further-integrating-telehealth-and-delivering-quality-care-for-veterans.html>
17. US Department of Veterans Affairs. VA Video Connect visits increase 1000% during COVID-19 pandemic. Accessed August 25, 2020. <https://www.va.gov/opa/pressrel/pressrelease.cfm?id=5467>
18. J.D. Power. Telehealth: best consumer healthcare experience you've never tried, says J.D. Power study. Accessed August 10, 2020. <https://www.jdpower.com/business/press-releases/2019-us-telehealth-satisfaction-study>
19. The White House. Executive order on improving rural health and telehealth access. Accessed September 8, 2020. <https://www.whitehouse.gov/presidential-actions/executive-order-improving-rural-health-telehealth-access>
20. Dolezel D, McLeod A. Cyber-analytics: identifying discriminants of data breaches. *Perspect Health Inf Manag*. 2019;16(Summer):1a. Accessed September 8, 2020. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6669366>
21. <https://www.usa.philips.com/healthcare/education-resources/publications/population-health-insights/case-studies/eastside-health-network-overcomes-integration-challenges>
22. <https://www.philips.com/a-w/about/news/archive/blogs/innovation-matters/2020/20200901-can-digitalization-support-a-circular-economy-and-sustainable-healthcare.html>
23. <https://www.usa.philips.com/a-w/about/news/archive/standard/news/press/2020/20200312-philips-becomes-first-medical-device-manufacturer-granted-new-underwriters-laboratories-product-cybersecurity-testing-firm-registration.html>

