PHILIPS

Position paper

Transforming barriers into enablers

How interoperability and cybersecurity are helping to deliver on the promise of connected care

We are entering a new era of opportunity in connected care

The pandemic has propelled health systems around the country to serve patients in new ways and in settings both inside and outside of the walls of the hospital. Securely connecting care across these settings is imperative, so providers have the complete picture of information they need to confidently care for their patients, so clinical and operational workflows are optimized, and so care delivery can be extended to reach patients when and where they need it.

By enhancing interoperability and cybersecurity, health systems have the opportunity to reach more people in more ways and more places than ever before.

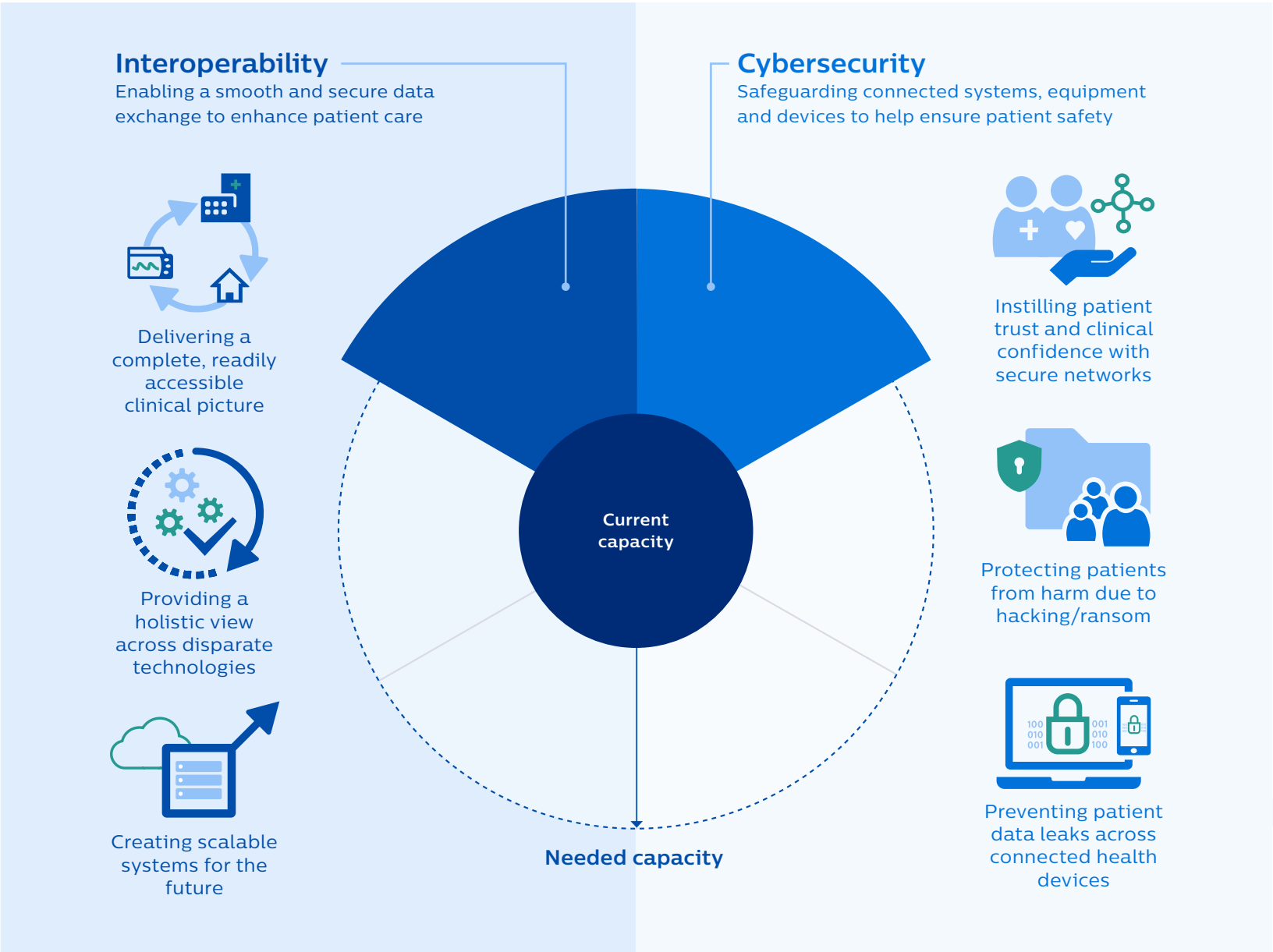
The expanding connected care landscape comes with challenges that demand secure, interoperable solutions

More settings	**More sites of care** With care expanding to other sites such as homes, community centers and even retail locations, patient information is spread across multiple systems, locations and formats. Without interoperability between care settings, devices and electronic health records (EHRs), vital patient information is lost and care teams lack a complete picture – **around 73% of physicians feel they have insufficient information about their patients**.[1]
More systems and devices	**More siloed systems** When systems operate separately, information is not readily available from one to the next, impacting patient care. Patients can, for example, end up staying in intensive care units (ICUs) longer than needed, resulting in overcrowding, delays in care, exposure to errors and financial consequences.[2] **More networked devices** With more and more connected technologies – from smartphones and wearables to pulse oximeters and maternal monitors – threats to information integrity and data security are growing every day. As a result, patient care may be impacted due to altered data, canceled surgeries, and even diverted ambulances.[3] **More bedside monitors** With **US hospitals averaging 10 to 15 connected medical devices per bed**, consolidating disparate data is a challenge.[4]
More people	**More providers interacting with data** Expanding care sites mean more people are interacting with patient data, leading to vulnerabilities and miscommunications; **80% of serious medical errors involve miscommunication among care teams during patient transfers**.[5]
More complexity and risk	**More health system mergers** Mergers have continued at a historic pace and appear even more strategically pressing as the pandemic recedes and liquidity crunches persist.[6] These mergers invariably require the integration of many disparate systems with various security standards. **More risk for cyberattack** In 2020, **the US healthcare industry saw a 25% year-over-year increase in data breaches**. Globally, individual breaches cost $7.13 million on average.[7,8]

Despite these challenges, health systems have the opportunity – increasingly, the imperative – to leverage the full benefits of interoperability to take their connected care strategy to the next level. Moving data securely across multiple platforms, systems and vendors requires a partner that takes a human-centered design approach when developing clinical solutions and services. Transforming interoperability and cybersecurity from potential barriers to enablers is essential for building a stronger healthcare system.

Connecting and securing data and systems to help improve patient care and safety

The future of connected care requires:



This paper argues why interoperability and cybersecurity are critical health system investments that require a proven partner to help increase clinical confidence, optimize clinical and operational workflows, and extend care delivery – all of which help close the capabilities and capacity gap, leading to improved patient care and safety.

Interoperability is critical in helping care teams identify gaps in care.

Enabling a smooth and secure data exchange to enhance patient care

Quality healthcare depends on patient information flowing seamlessly as a patient moves from setting to setting – from home to the emergency department (ED) to the ICU to the med/surg unit and beyond.

However, managing multiple vendors and equipment can be complicated, holding health systems back from realizing the true potential of their technology. Interoperability solutions can help enable this smooth and secure exchange of data within a single team and from one team to the next, fostering greater clinical confidence, optimizing both the clinical and operational workflows in care delivery and, ultimately, improving patient care. As an example, Philips integrated platform of acute patient management solutions provides continuous surveillance, embedded data analytics, advanced interoperability and smart services to deliver clinically valuable insights to all points of care. In fact, one of our secure, vendor-agnostic interoperability solutions is at work across 1,500+ hospitals with more than 300 third-party device models from 65+ manufacturers supported to collect, distribute and amplify critical data across the care continuum.[9,*]

Delivering a complete, readily accessible clinical picture

Interoperability helps ensure that providers in a wide range of care settings have ready access to patients' complete clinical pictures. This can result in less duplication and waste and can help providers identify any gaps in patient care for improved health outcomes.[10] Interoperability between clinical solutions and EHRs also makes it possible for clinical teams to utilize advanced analytics to make the timely decisions their patients require, moving them to a lower- or higher-acuity care setting as needed. And interoperable systems increase the likelihood that an ever-changing care team is working from the same set of information, avoiding the dangers that result from miscommunication when patients are transferred between settings. At Saratoga Hospital, the staff leveraged a Philips early warning score protocol that streamlines the otherwise manual process of entering vitals into the EHR. By automating scoring, clinicians can better spot vital sign deviations, allowing clinical teams to intervene hours before a potential adverse event occurs. Philips interoperability solutions link this technology to the EHR so patients' vital sign information is sent directly into the EHR to be assessed. Fewer manual processes and more seamless flow of data enables earlier deterioration detection and intervention. In fact, Saratoga Hospital saw a 63% reduction in patient transfers to the ICU.[11,**]

Providing a holistic view across disparate technologies

When partnering with a health system to improve interoperability, Philips works with a customer's specific needs and goals to implement a platform that brings their unique systems together, synching legacy systems with new solutions as needed. Philips is helping to make interoperability possible for the US Department of Veterans Affairs (VA), who needed technologies and data to work securely across a broad range of geographic settings and devices. See customer story on page 8.

*Philips IntelliBridge Device Interface Library document and Philips internal sales data.
**Results are specific to the institution where they were obtained and may not reflect the results achievable at other institutions.

Interoperability is driving COPD management by helping patients avoid readmissions.

Creating scalable systems for the future

Care delivery is rapidly expanding beyond the doctor's office and beyond hospitals to virtual care and telehealth visits in homes, community centers, retail settings and other medical facilities, providing services such as remote screening and triage and proactive management of patients in low-acuity and lower-cost settings. Interoperability amplifies the impact of data from multiple sources, such as remote patient monitoring (RPM) and diagnostic medical devices, allowing a provider to view patient records and real-time RPM or device data during visits. At the same time, health systems need to securely share data with everyone from patients and providers to families and proxies, requiring accurate identification of the patient, stringent access permissions and granular controls. Interoperability solutions resolve current data-sharing issues and can be tailored to expanding needs.[12]

Additionally, caring for patients with chronic illnesses will continue to be a pressing need, and supporting these patients and their caregivers with connected devices, RPM and customized clinical pathways to detect deterioration can enable providers to intervene earlier, reduce costs and reduce readmissions. And for family members/caregivers, these solutions can help ease their burden and empower them with information. Interoperability is imperative to powering these solutions.

Today, many patients with chronic conditions are not well managed, which leads to suboptimal outcomes and higher costs. In one study, 71% of moderate-to-severe COPD patients from a Medicare population study did not receive maintenance pharmacotherapy.[13] Interoperable solutions can help.

Interoperability helped power Philips Integrated COPD Care Initiative

Using continuous data collection to identify gaps in care, Philips Integrated COPD Care Initiative reduced COPD readmissions and costs in less than one year.[14,*]

80% reduction
in acute 30-day readmissions

$1.3 million
saved in acute 30-day readmissions

>70% reduction
in all-cause diagnoses readmissions

$4.4 million
saved in all-cause diagnoses readmissions

Philips Integrated COPD Care Initiative – powered by evidence-based care strategies, care coordination pathways and robust data and analytics – can help better manage the care of patients with COPD.[14]

*Results are specific to the institution where they were obtained and may not reflect the results achievable at other institutions.

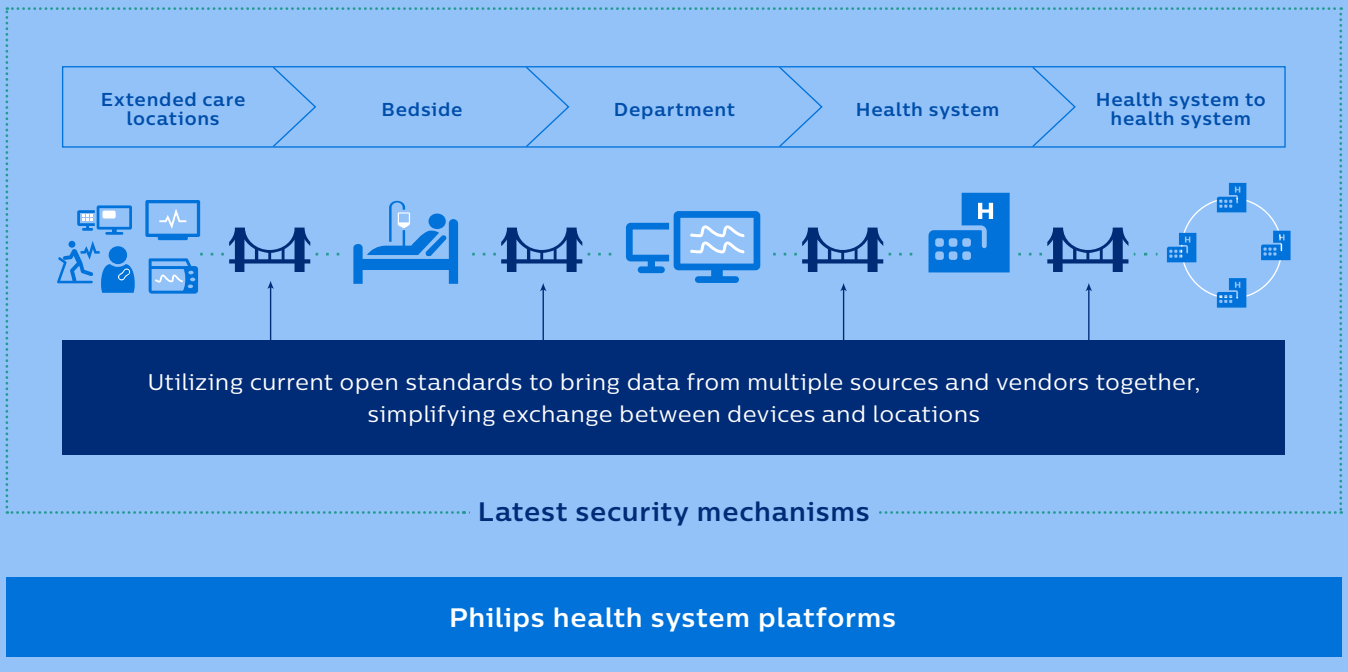
Helping to advance interoperability standards for the healthcare industry

Philips is highly invested in not just meeting current standards but raising the bar and contributing to the evolution of industry standards.

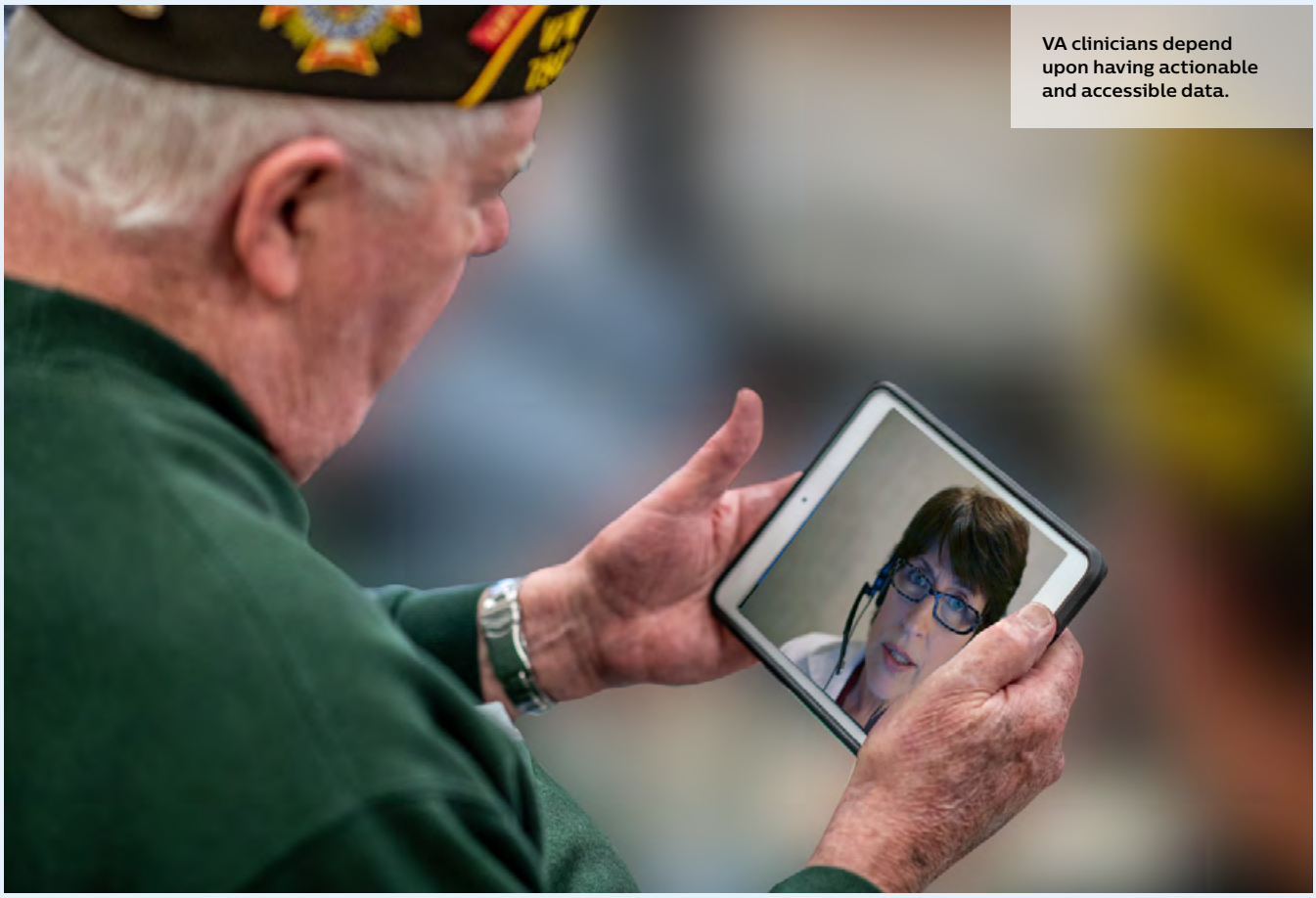
Philips participates in the Global Consortium for eHealth Interoperability, where we advocate to make policy-based interoperability road maps a reality. We were also an early adopter of HL7's Fast Healthcare Interoperability Resources (FHIR) specification, a standard for organizing and describing healthcare data for ease of exchange between systems. This gives us perspective on how the healthcare industry will adopt new standards and allows us to anticipate how legislation like the 21st Century Cures Act will affect a customer's interoperability needs.

A health system where smooth data exchange occurs across points of care is a system that is easier to secure against malicious online attacks. As health systems expand and merge, a confluence of multiple technologies and processes across settings – each using a different standard of measuring security – complicates the work of administrators. Improving the interoperability of systems establishes a common, well-defined standard for managing data security across the health system, enabling administrators to more easily build for the future.

Philips interoperability solutions help make seamless care connections



Case study: US Department of Veterans Affairs



VA clinicians depend upon having actionable and accessible data.

Connecting care for the country's largest health network

Veterans Health Administration (VHA) is the largest federal health system

As part of VA, VHA provides healthcare to nearly nine million veterans across 18 regional Veterans Integrated Service Networks, 171 medical centers, more than 1,000 Community Outpatient Centers and several hundred Veterans Centers, Mobile Vet Clinics, and Access Telehealth Local Area Stations locations.[15]

Maintaining such a large and vital network comes with challenges, which were worsened by the pandemic

Roughly five million veterans live in areas designated as rural by the US Census Bureau,[16] making access to healthcare difficult. And as that population ages, the prevalence of chronic conditions is projected to rise. By 2060, the number of US adults with diabetes is projected to nearly triple from 39.7 million to 60.6 million.[17] Difficulty in accessing care was exacerbated during the pandemic, when patients needed to receive care from home and when reduced rates of admission for heart attacks, strokes and other emergencies suggested that patients may have been avoiding necessary care out of a fear of going to the hospital.[18] In 2020, there was a 56% decline in in-person visits across VA outpatient facilities, which was only partly offset by the twofold increase in the number of telephone and video visits.[19]

VA extended care via a virtual health solution

To combat these trends, enhance the experience of veterans, caregivers and survivors, and make healthcare as accessible and efficient as possible, VA utilized a virtual health solution that extended access to care, helped to coordinate team members and facilitated the secure and seamless flow of data across devices and locations.

Untethering patients from a centralized location

To make device- and setting-agnostic care possible, VA partnered with Philips prior to the pandemic to better understand VA's clinical needs, assess the existing level of interoperability, understand documentation requirements and, ultimately, provide the equipment for virtual care stations within Veterans of Foreign Wars and American Legion posts throughout the United States. With this virtual health solution in place, VA was prepared to respond and meet the needs of veterans throughout the pandemic.

Keeping patients healthier outside the hospital

This allows care to be delivered in more accessible and comfortable settings, such as the home, helping VA to improve the care experience, consistency of care and focus on preventative care to keep patients healthier outside the hospital. In the event patients move between care settings, VA can ensure that they are better served throughout their journey. Veterans' satisfaction with their care ultimately improved, due in part to the many components and data that work seamlessly together across time and place.[20,*]

Cybersecurity protects these evolving care connections

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, VA again partnered with Philips, working closely throughout the enterprise risk assessment (ERA) process and preparing to conduct the Federal Risk and Authorization Management Program (FedRAMP):

- Addressing potential material weakness in network-connected devices by identifying the inherited risk and impact
- Addressing system-specific security controls
- Managing and addressing vulnerabilities

And because of our commitment to interoperability, Philips technology, such as 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.

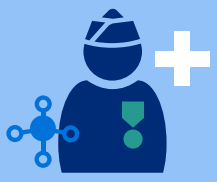
By working with partners like Philips to conceive the patient journey as an interoperable virtual care solution, VA is helping to secure the future of patients' health and the integrity of its continuum of care. In the future, VA will be tasked with serving more veterans with greater need. The connected care solutions now in place are secure and scalable, ready to face the evolving needs and changing dynamics of this population. Learn more about our work with government agencies.

Expanding access to care

Leveraging interoperability to make telehealth possible for veterans

18+ million

people cared for by VA and the DoD's Military Health System, making these two of the nation's largest and most complex health systems[15,21]



9 million

veterans enrolled in the VA healthcare system, including three million living in rural areas[22]

2.5+ million

VA video telehealth visits facilitated in 2019, a record for VA[23]

1000% increase

in VA video telehealth visits during the first weeks of the COVID-19 pandemic[24]

DoD=Department of Defense.
*Results are specific to the institution where they were obtained and may not reflect the results achievable at other institutions.

Partnering to drive continuous improvement

Manage multiple systems with one point of contact

Wrangling the complexity of a vast array of medical technology can be challenging. Reworking technologies to be interoperable, along with introducing new technologies and maintaining security, makes this even more complex. This is where companies like Philips who can work across multiple systems play a role in providing vendor-agnostic solutions.

Instead of dealing with a large number of contracts from various vendors, Philips can act as one source for providing staff training and education, managing medical technology equipment and life cycle, and optimizing cost and performance, all with an eye on enhancing interoperability and cybersecurity across the board.

Philips offers vendor-agnostic, multimodality solutions for maintenance, life cycle and performance services for imaging and biomedical assets. Our solutions are designed to cost-effectively manage clinical assets across one or multiple sites of care, helping to simplify data and insight gathering, drive operational excellence and enhance the patient and staff experience.

As health systems seek to improve interoperability and cybersecurity, they should look for strategic partners who can help:

- Standardize vendors/service providers
- Optimize staff training to keep up with changing technology
- Realize the greatest return and value from capital assets
- Maximize throughput and efficiency
- Improve profitability and lower costs

Protecting patient lives by securing devices, systems and networks

Safeguarding connected systems and devices to help ensure patient safety

Health data breaches and malicious online attacks like ransomware are arguably two of the biggest worries keeping healthcare leaders up at night.[7] The healthcare industry in particular is being targeted by attackers.[25]

As health systems extend more care into communities and homes, they 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.[26]

Cybersecurity attacks can harm patients.[3] Those attacks also can have a lasting impact on the security of a health system's infrastructure, the interoperability of medical devices and clinical systems, and the integrity of patient data. It is imperative that health systems partner with a health technology and service provider well versed in cybersecurity that is prepared to make sure all devices, systems, networks and data are not only interoperable but protected, so patient lives are not harmed or lost and health systems can continue providing value-based care to the communities they serve. In order to get ahead of cybersecurity risk, health systems must first identify the source. Read on to learn more.

"The digitization of healthcare presents both opportunities and threats... Assuring the integrity of these devices, systems and associated data requires a cohesive cybersecurity program based on comprehensive risk assessment and robust implementation."[27]

–Gal Gnainsky, VP, Chief Security Officer, Philips

Spotlight: getting to the source of risk

Identifying the source of cybersecurity risk is necessary for staying ahead of it.

Where do your cybersecurity risks lie?

Cybersecurity is often a moving target. Health systems are under tremendous pressure to stay ahead of cyberattacks, but the inherent complexities, talent shortages and lack of a standardized playbook for keeping systems current also pave the way for vulnerabilities. Addressing those vulnerabilities requires the optimal mix of human and technical resources to achieve a full understanding, both granular and broad, of the challenges presented and potential impact. To put it simply, if you are not informed, you are at risk. In order to mitigate threats, healthcare leaders must not only recognize their level of risk but the cause of it. Philips understands the risks facing health systems today and can help identify and address those risks.

Potential outcomes of common organizational cybersecurity risks

Organizational risk	Potential outcome
Lack of embedded security requirements in application development as well as **lack of security parameters** in hosted websites	**Security breach** via abuse of vulnerabilities in software and websites
Lack of governance to handle the privacy of sensitive information collected during the course of business operations	**Loss of information from security breach** and violation of compliance requirements
Weak identity credential and access management (including failure to implement proper access, inconsistent review of user access and timely removal of access rights) and **failure to implement two-factor authentication**	**Unauthorized access** or leakage of critical information
I**nsecure decommissioning of IT assets/medical devices** – including nonremoval of configuration, authentication and other information from assets prior to disposal	**Loss of organization's information assets**
Failure to incorporate minimum security requirements in information systems, such as password management hardening, vulnerability management and secure network zoning	**Security breach** on IT assets
Inadequate incident response infrastructure (e.g. plans, defined roles, training, communications and management oversight) for quickly discovering a cyberattack	**Delay in eradicating the attacker's presence, containing cyberattack damage and restoring integrity** of the network and systems
Inadequate backup of information from end-user devices and enterprise-grade servers/databases	**Failed continuity of business operations** during a crisis due to nonavailability of information

Philips can help organizations uncover cybersecurity vulnerabilities and implement best practices based on our extensive experience working with complex government agencies and health systems large and small. Our expertly trained and certified consultants can partner with your in-house staff to conduct organizational security assessments and provide actionable recommendations based on a globally recognized risk framework. We bring together the knowledge, resources and competencies to deliver a truly scalable approach to cybersecurity that helps empower our customers' digital transformation.

Instilling patient trust and clinical confidence with secure networks

Now that care connects across more devices and to more places, patients want to be assured that their sensitive personal information will not be compromised.[28] If in doubt, patients may stop participating in vital connected care services, such as at-home monitoring or telehealth follow-up visits, or may seek care elsewhere. Providers also need to feel confident that patient data is secure and that they have the most up-to-date information so they have the clinical confidence they need to effectively diagnose and treat their patients and their workflows are not disrupted by missing or compromised information.

Protecting patient lives from harm due to hacking/ransom

The potential for patient harm when a poorly protected health system is hacked or ransomed is staggering. All the systems that support patient care can actually become a danger to patients when a health system is under attack and data is ransomed. For example:

- Ambulances rushing critical patients to a hospital may be diverted, potentially impacting outcomes.
- Surgeries may be canceled, putting patient lives at risk.
- Pharmacy, medication information and EHR access may be blocked, leading to errors.
- Compromised lab systems can stop care in its tracks.
- Communication systems may be shut down, preventing care teams from sharing information.

While protecting patients is the priority, health systems, too, can face other serious issues. Huge financial setbacks are difficult to recover from, and fines related to leaked data are also costly. Highly publicized incidents can mar the image of the health system, damaging its reputation and brand value. Patients may lose trust and may move to competitors they feel are more secure.

Philips robust cybersecurity approach takes into account the ever-present threats to data and system security – threats that are made all the more complex by the many entry points to data and systems and the evolving hacking and ransomware scenarios that health systems face. Philips Cybersafe puts a patient focus first and works to ensure the confidentiality, integrity and availability of the data on which patient care and patient lives depend.

Preventing patient data leaks across connected health devices

As connected care expands, the possible points of entry keep expanding as well. Healthcare IT leaders need solutions that deliver on their core clinical value but are also backed by a manufacturer who is committed to the understanding that the minimum requirements for security are just the starting point. Philips is committed to the deployment of comprehensive security plans that assure the safety of medical devices, business enterprise information and personal data, so health system leaders can be secure in the confidentiality, integrity and availability of critical data and the systems that house it. Philips HealthSuite Digital Platform (HSDP), a curated marketplace of foundational cloud services, supports many of our connected solutions. In fact, HSDP is responsible for connecting approximately 11 million internet of things (IoT) devices and has helped health systems securely archive 145 billion images and 30 petabytes of imaging studies. HSDP delivers increased security and privacy by reducing dependency on local hardware to store sensitive data, utilizing cloud providers dedicated to data and privacy protection and providing automated software updates so systems stay current.[29]

Read why cloud-based platforms should be a key priority for healthcare leaders in a post-pandemic world.

HSDP supports secure data connections across a number of health applications[29]

~11 million IoT devices connected

145 billion images archived

30 petabytes of imaging studies archived

In the complexity of healthcare today, health systems need end-to-end security

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. Philips Cybersecurity Services comprise an end-to-end suite of technologies and services to safeguard medical systems, devices and related software solutions regardless of their manufacturer.

Our cybersecurity approach is aligned with recognized standards such as NIST 800-53, ISO/IEC-27000 series, and HITRUST. In 2020, Philips became the first medical device manufacturer to receive a new Underwriters Laboratories (UL) product cybersecurity testing certification. We have long been committed to the ongoing effort to continuously improve our processes and systems to minimize the risk to patients who depend on our solutions and services.[30]

Security by design is an end-to-end mindset

Security principles, requirements and controls are addressed at and integrated into all aspects of the secure development life cycle. This starts with product design and development, continues through testing and deployment, and is followed with robust policies and procedures for monitoring, effective updates and, where necessary, incident response management.[31]

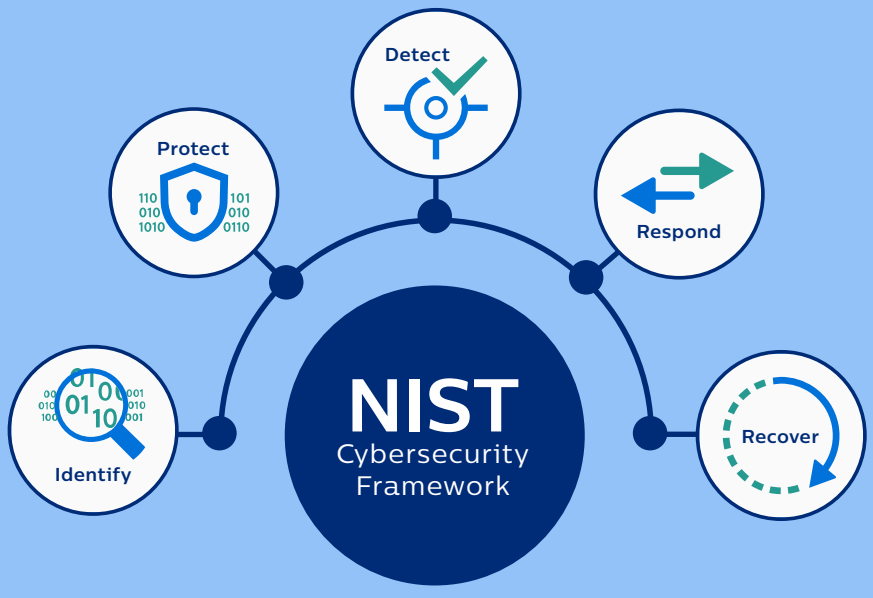
- **Accountability**
  Cybersecurity is built in from the very start. Our products are aligned with recognized security programs, policies and standards. And continuous product security training occurs across the Philips organization.
- **Risk assessment**
  We conduct rigorous risk assessments of our products and services.
- **Security testing**
  We subject our products to rigorous verification and validation methods to assure that high standards of safety, security, efficacy, quality and performance are met in all products and services.
- **Transparency**
  We take responsibility and collaborate transparently with regulatory agencies, industry partners, healthcare providers and others to close security loopholes and implement safeguards.

Partnering to support comprehensive cybersecurity

Philips Cybersecurity Services are supported by a partnership with CyberMDX, a leading provider of healthcare cybersecurity capabilities for hospital digital environment mapping and evaluation, medical device risk assessment, threat detection and intelligence, and related support. Data and insights collected through CyberMDX form a core foundation for development and implementation of a full cybersecurity plan for individual customers.[27]

Philips follows the NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides guidance on how to be better prepared in identifying, detecting and responding to cyberattacks.

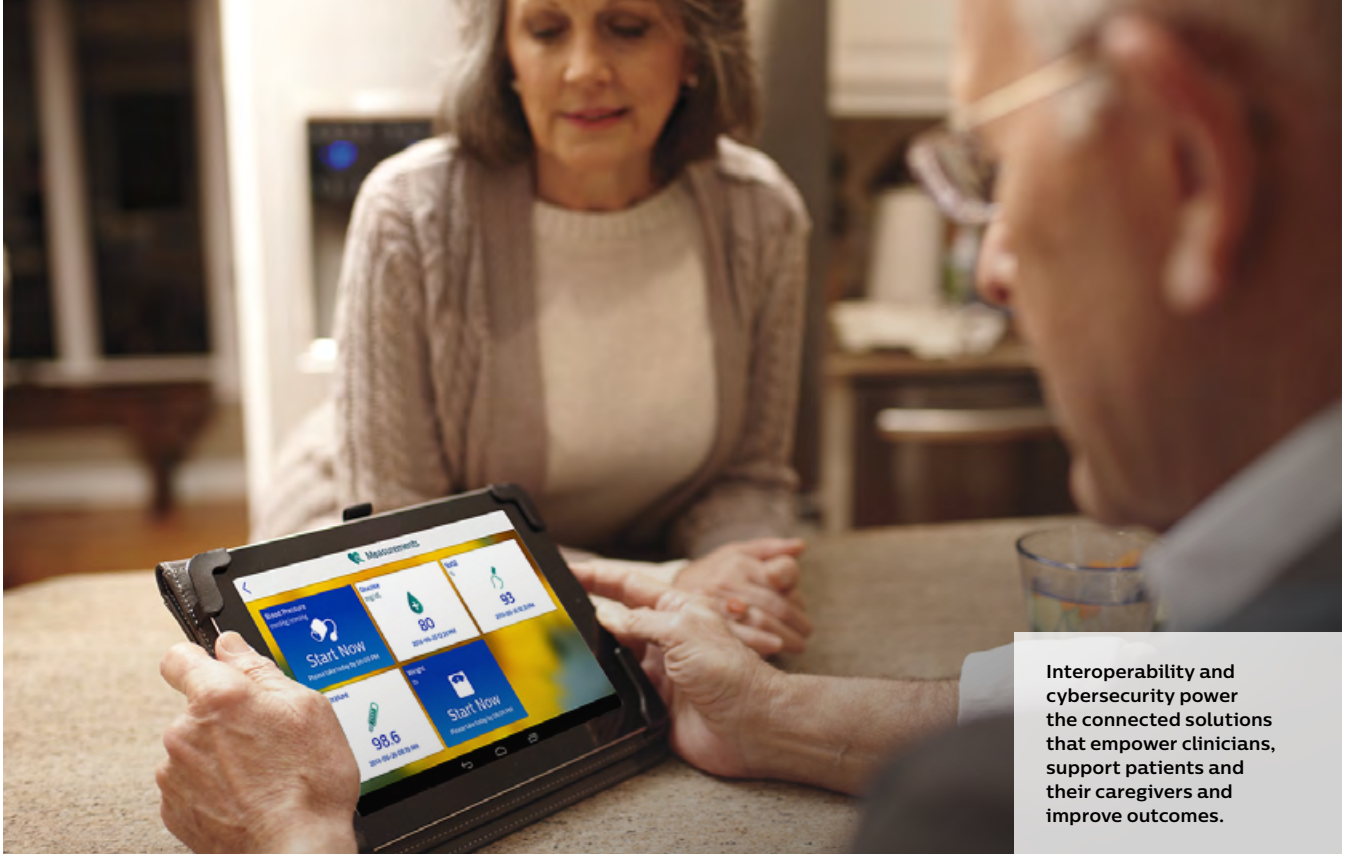


Spotlight: Department of Defense

Cybersecurity that performs to US government specifications.

Our security services meet the high standards of the DoD

The DoD sets a high standard when it comes to cybersecurity and understandably so. A data breach for our nation's military could expose classified information, impacting the military's readiness and effectiveness, potentially putting our service members, government leaders and population at risk. 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 VA's ERA process. By performing to these specifications, Philips can better enable the systemwide availability and cybersecurity of patient data and diagnostic images for clinical staff, thereby facilitating more timely and effective care.



Interoperability and cybersecurity power the connected solutions that empower clinicians, support patients and their caregivers and improve outcomes.

Summary

Health systems must continue to expand capacity and capabilities to untether caregiving from physical locations and extend care to where patients live and work.

As we build new and better systems for the future, we need to transform interoperability and cybersecurity from potential barriers to enablers that can drive the efficiency, effectiveness and safety of care for patients. Interoperability and cybersecurity are deeply connected. The promise of true interoperability is allowing patient care teams to perform at their best by ensuring they have trusted data at their fingertips – whenever they need it, wherever they are. This promise can only be met when interoperable systems are paired with robust cybersecurity, keeping patients and their data safe and instilling confidence in both patients and caregivers.

Achieving your interoperability and cybersecurity goals requires a partner who understands the complexities and challenges you face and who can cut through the clutter so you have one point of contact helping you manage multiple systems. At Philips, we apply a human-centered design approach to every solution, paying careful attention to the bigger picture and the ways in which each solution serves to both connect and secure the data and systems on which healthcare depends. Together, we can improve interoperability and cybersecurity across growing health systems to enhance care delivery for patients, keep patients safe, improve caregiving experiences for clinical teams and make health systems stronger.

This guide showcases how Philips connects and secures data and systems to improve patient care and safety.

Subscribe for updates

“Until we really see the consumer at the center of the experience, then all these solutions and technologies we wrap around people will be missing that human element.”

– Kristine Mullen, Head of Marketing, Connected Care at Philips, March 2021 IHE North American Connectathon Conference

References

1. Quest Diagnostics. *Stalled Progress on the Path to Value-Based Care: A Survey of Physicians and Health Plan Executives*. 2018. Accessed April 26, 2021. http://images.health.questdiagnostics.com/Web/QuestDiagnosticsIncorporated/%7B67d434a3-0cbf-4683-b5f2-853179755911%7D_Quest_2018_VBC_Study-min_(1).pdf

2. Blanch 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.

3. Riggi J. The importance of cybersecurity in protecting patient safety. Accessed April 21, 2021. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety

4. CyberMDX. *The Big Healthcare CIO Factbook*. HIMSS 2020. Accessed April 26, 2021. https://himss20.mapyourshow.com/8_0/explore/collateral_redirect.cfm?CollateralID=4411&CFID=722107&CFTOKEN=7ea7b376536fb8e6-86BD09C6-FAFD-FC20-0898D320994719F9

5. Joint Commission Center for Transforming Healthcare releases targeted solutions for hand-off communications. *Jt Comm Perspect*. 2012;32(8):1, 3.

6. Kaufman Hall. 2020 M&A in review: COVID-19 as catalyst for transformation. Accessed April 21, 2021. https://www.kaufmanhall.com/ideas-resources/research-report/2020-mergers-acquisitions-review-covid-19-catalyst-transformation

7. HIPAA Journal. 2020 healthcare data breach report. Accessed April 5, 2021. https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

8. IBM News Room. IBM report: compromised employee accounts led to most expensive data breaches over past year. Accessed April 21, 2021. https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year

9. https://www.usa.philips.com/healthcare/resources/landing/acute-patient-management

10. US Centers for Medicare & Medicaid Services. Interoperability and patient access fact sheet. Accessed May 19, 2021. https://www.cms.gov/newsroom/fact-sheets/interoperability-and-patient-access-fact-sheet

11. https://www.usa.philips.com/a-w/about/news/archive/standard/news/press/2018/20180307-saratoga-hospital-partners-with-philips-to-improve-patient-care-and-safety.html

12. https://www.usa.philips.com/healthcare/resources/landing/interoperability-solutions#triggername=close_it

13. Make B, Dutro MP, Paulose-Ram R, Marton JP, Mapel DW. Undertreatment of COPD: a retrospective analysis of US managed care and Medicare patients. *Int J Chron Obstruct Pulmon Dis*. 2012;7:1-9.

14. https://www.usa.philips.com/c-dam/b2bhc/master/education-resources/copd-insider/common/alabama-paper/the-integrated-copd-care-intitative-copd-insider.pdf

15. Veterans Health Administration. About VHA. Accessed April 21, 2021. https://www.va.gov/health/aboutvha.asp

16. Holder KA. Veterans in rural America: 2011-2015. United States Census Bureau. Accessed April 21, 2021. https://www.census.gov/content/dam/Census/library/publications/2017/acs/acs-36.pdf

17. Lin J, Thompson TJ, Cheng YJ, et al. Projection of future diabetes burden in the United States through 2060. *Population Health Mtr.* 2018;16(9):1-9.

18. Krumholz HM. Where have all the heart attacks gone? *The New York Times*. April 6, 2020. Accessed April 5, 2021. https://www.nytimes.com/2020/04/06/well/live/coronavirus-doctors-hospitals-emergency-care-heart-attack-stroke.html

19. Baum A, Kaboli PJ, Schwartz MD. Reduced in-person and increased telehealth outpatient visits during the COVID-19 pandemic. *Ann Intern Med*. 2021;174(1);129-131.

20. Slightman C, Gregory AJ, Hu, J, et al. Patient perceptions of video visits using Veterans Affairs telehealth tablets: survey study. *J Med Internet Res*. 2020;15:22(4):e15682.

21. Military Health System. Beneficiary population statistics. Accessed August 10, 2020. https://www.health.mil/I-Am-A/Media/Media-Center/Patient-Population-Statistics

22. VA Office of Rural Health. Rural veterans. Accessed August 10, 2020. https://www.ruralhealth.va.gov/aboutus/ruralvets.asp

23. 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

24. US Department of Veterans Affairs. VA Video Connect visits increase 1000% during COVID-19 pandemic. Accessed April 21, 2021. https://www.va.gov/opa/pressrel/pressrelease.cfm?id=5467

25. Seh AH, Zarour M, Alenzi M, et al. Healthcare data breaches: insights and implications. *Healthcare (Basel)*. 2020;8(2):133.

26. Dolezel D, McLeod A. Cyber-analytics: identifying discriminants of data breaches. *Perspect Health Inf Manag*. 2019;16(Summer):1a.

27. https://www.usa.philips.com/a-w/about/news/archive/standard/news/press/2020/20201130-philips-expands-its-healthcare-customer-services-portfolio-with-the-introduction-of-integrated-cybersecurity-services.html

28. Eddy N. Data privacy concerns hamper adoption, use of personal medical devices. Healthcare IT News. Accessed April 30, 2021. https://www.healthcareitnews.com/news/data-privacy-concerns-hamper-adoption-use-personal-medical-devices

29. https://www.usa.philips.com/c-dam/b2bhc/master/hts/healthsuite/pins-e-1.PDF

30. 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

31. Philips Healthcare YouTube page. Responding to imminent cybersecurity threats in healthcare: Philips HIMSS 2020. Accessed May 25, 2021. https://www.youtube.com/watch?v=7p4YiBX-B_k

philips.com/interoperability-cybersecurity