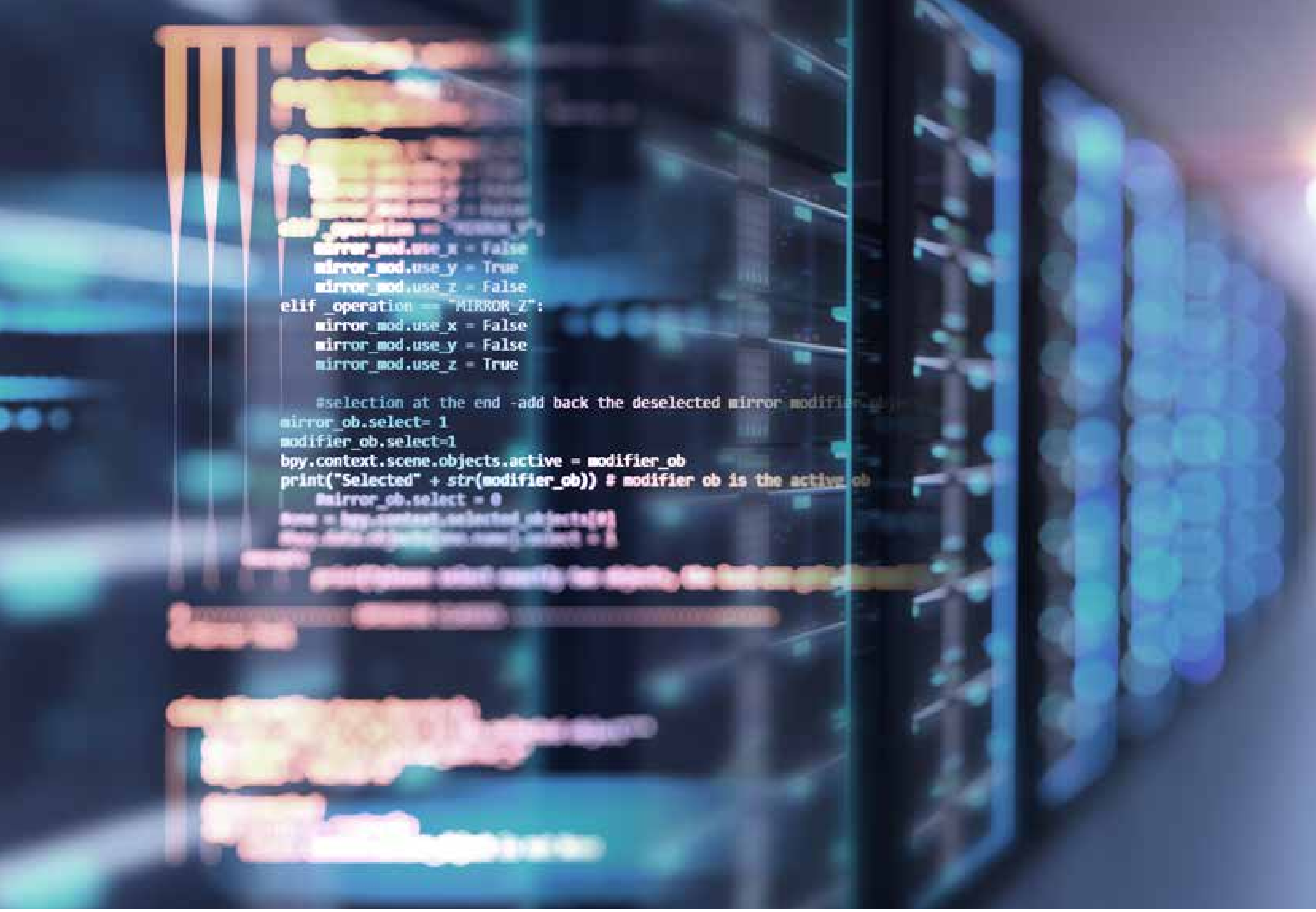
PHILIPS

Services and solutions delivery

Operational Intelligence

Critical data, end-to-end security

Executive briefing



```
        mirror_mod.use_x = False
        mirror_mod.use_y = True
        mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
        mirror_mod.use_x = False
        mirror_mod.use_y = False
        mirror_mod.use_z = True

        #selection at the end -add back the deselected mirror modifier obj
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
        #mirror_ob.select = 0
```

The medical device cybersecurity imperative

> Data is the new currency, and hacking is a business model. The financial gains of hacking will soon surpass those of the worldwide drugs trade.”
>
> Stef Hoffman, Chief Information Security Officer, Philips

Within the complex, transforming healthcare system, there is a highly specific area of cybersecurity that goes beyond the arena of IT and demands specific health systems expertise, such as that only able to be provided by expert health informatics and device manufacturers, such as Philips.

This rapidly evolving, highly regulated and vital niche is known as medical device cybersecurity and it’s a subject about which every change-maker senior leader needs to know now, since it is key to operational effectiveness.

After all, if 81% of healthcare organizations had their data compromised by a cyber attack[1] between 2013 - 2015, according to a report by KMPG. Amidst the global coronavirus pandemic and 5 years on as healthcare continues to become a system of engagement, just imagine the scale of the potential threat today.

[1] Between 2013-2015 as reported in a 2015 report from KPMG

What is medical device cybersecurity?

Networked medical devices and other mobile health technologies are a true double-edged sword: They have the potential to play a transformational role in health care but also may be a vehicle that exposes patients and health care organizations to safety and security risks.

In today's increasingly connected healthcare landscape, hundreds of thousands of medical devices such as patient monitors, infusion pumps, ventilators, and imaging modalities – many of which are life-sustaining or life-supporting – currently reside on hospital networks across the world. Even more medical devices are accessible via wireless technologies, for example, insulin pumps and pacemakers.

Effective medical device cybersecurity – such as the strategies and offerings provided by Philips – is an end to end security offering that complies with and builds upon global regulations to make medical device products and services robust against cyber threats.

Philips medical grade cybersecurity solutions encompass the provision of an on-site biomed and security (people) backed by Philips Group security processes (process), and enabled by technology specifically selected for healthcare. This unique combination reflects our Operational Intelligence approach to integrating people, process and technology at all levels of operations, in this case cybersecurity to ensure security excellence and continuous improvement.

As Gal Gnainsky, Head of Phillips Group Security strongly emphasizes: "Patient safety in today's connected care environment is a task we take incredibly seriously.
As we evolve our cybersecurity programs, transparency, accountability and responsiveness must be priorities we continue to maintain."

What constitutes a medical device?
The Food and Drug Administration (FDA) defines a medical device in section 201(h) of the Federal Food Drug & Cosmetic (FD&C) Act as: "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is: - recognized in the official National Formulary, or the United States Pharmacopoeia, or supplement to them; - intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals; or - intended to affect the structure or function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes."

As defined above, a medical device is regulated by the FDA and is subject to pre-marketing and post marketing regulatory controls. In 2011, the FDA issued the Medical Device Data System (MDDS) rule, which clarified medical device regulation to include software, electronic or electrical hardware (including wireless) that makes claims to be useful for the medical purposes described in the MDDS classification (i.e., not generic software).

The MDDS classification covers systems that act as a mechanism to transfer, store, convert, or display medical device data without controlling or modifying the function or parameters of a connected medical device.

Software that meets the law's definition of "medical device" in the United States has been subject to FDA scrutiny for safety and effectiveness. To date, the FDA has regulated software under the quality system regulation; however, with more focus on the security of such systems, as evidenced by the draft guidance on cybersecurity, this may be changing.

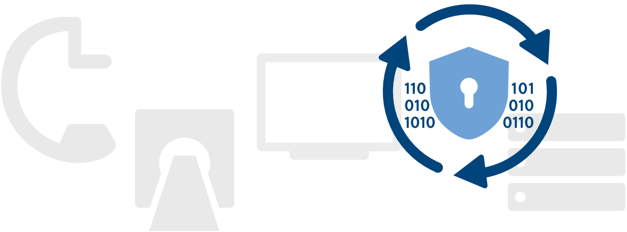
What is not a medical device?
Both EU and FDA definitions of devices exclude fitness, lifestyle and wellbeing devices and applications. These may be considered as mHealth products: mobile health, utilizing connected mobile platforms such as mobile phones and tablets to run health applications. mHealth is considered a sub-segment of eHealth (electronic health), using information communications technology (ICT). Regulations have not kept pace with the rapid developments however and work is ongoing in Europe to determine a suitable legal framework. Meanwhile, the UK National Information Board Work Stream 1.2 road map is developing an assessment framework for digital applications. The UK Medicines & Healthcare products Regulatory Agency provides comprehensive device determination guidance flow chart in the medical device stand-alone software including apps document.

Why is effective, always-on medical device cybersecurity vital to operational effectiveness?

In a 2012 episode of the popular television series Homeland, the Vice President of the United States was assassinated when a terrorist organization wirelessly hacked his pacemaker. While this scenario may seem far-fetched, there have been increasing real-life examples of medical devices being exposed and utilised for intentional threats (for example, insulin-pump hack) highlight concerns about cybersecurity threats to networked medical devices.

The sensitive and private nature of patient data has made cyber security a particularly important issue in the medical device industry. Today, medical devices are no longer simply machines attached to or used by the patient. Rather, they are often connected to the EHR—either hardwired or wirelessly and a typical ICU patient could easily be connected to ten or more networked devices.

While the information on the medical device may not be useful to a hacker, the medical device can be used as a conduit for accessing sensitive patient information, such home address and other forms of identification, which could be used for identity theft or real theft while the patient is hospitalized. Potential threats in medical devices include the physiologic monitor that runs on an outdated operating system, the ventilator with a USB port, and usernames and passwords for the vendor's field service engineers and in-house technicians that are hard-coded.



High profile incidents have brought medical devices under scrutiny

Several high profile incidents have brought medical device cybersecurity to the forefront of COO and senior leader concerns. For example, the global ransomware event known as WannaCry – and other attacks such as Petya/NotPetya - demonstrated how the performance of vulnerable medical devices may be compromised by an exploit, whether it intentionally targets the healthcare system or is purely opportunistic. A device infected with malware has the potential to shut down hospital operations, expose sensitive patient information, compromise other connected devices and harm patients.

Potential threats include:

- Electromagnetic interference
- Untested or defective software or firmware
- Misconfigured networks or poor security practices
- Failure to install timely manufacturer security software updates and patches to medical devices11 and concerns about causing service disruptions to functional device
- Uncontrolled distribution of passwords, such as employee carelessness in leaving a password unattended in public
- Disabled passwords, or hard-coded passwords for software intended for privileged medical device access (e.g., to administrative, technical, and maintenance personnel)
- Network transfer (via email, remote access channel, or file transfer)
- Unauthorized device setting changes, reprogramming, or infection via malware
- Targeting mobile health devices using wireless technology to access patient data, monitoring systems, and implanted medical devices
- Disruption of care/service (including potential for patient deaths) e.g.
- Deception of staff with spoof email or fake websites to obtain login credentials or install malware
- Spyware and malware
- Spearphishing attack
- Theft or loss of networked medical devices (external or portable)
- Unintentional or intentional 'Insider threat', which can pose a significant threat due to the position of trust within an organization
- Loss of patient information – especially electronic protected health information (ePHI)
- Data breach, information exfiltration and loss of assets
- Manipulation, theft, destruction, unauthorized disclosure, or lack of patient data availability to providers
- Blackmail, extortion and duress through exploitation of exfiltrated sensitive data e.g. Denial-of-service attacks
- Security and privacy vulnerabilities

Intellectual Property (IP) theft Research has shown that healthcare cybersecurity continues to focus on the protection of patient health records, whilst failing to address the real threats to, or adequately protect patient health and report on cybersecurity threats and events. Cybersecurity vulnerabilities can emerge in any medical device that can be connected to another electronic device or network.

High profile medical device cybercrime cases:

In 2017, the WannaCry cyber-attack targeted computers across the world using Microsoft's Windows system, encrypting people's data and demanding payments in the cryptocurrency Bitcoin before allowing access to it. Ransomware attacks like this involve cyber criminals threatening to publish the victim's data, or deny access to it unless a financial sum is paid. The hackers behind WannaCry cancelled tens of thousands of GP appointments and diverted NHS ambulances away from the destinations they were heading to.

In 2017, US based, MedStar Health, received bitcoin demands following encryption of computer systems. Notifications were displayed on infected computers, threatening loss of data after 10 days. Patient records for 10 hospitals and 250 outpatient centres were reported to be either unavailable and or could not updated, whilst MedStar used backups to restore data. Patient operations were cancelled and ambulances diverted. Nurses and doctors highlighted safety issues concerning delays to test results affecting treatment.[2]

In April 2018, the FDA recalled two of American healthcare company Abbott's defibrillator models after finding a potential vulnerability in their cyber security systems. In early 2019, an Israeli research group at the Ben-Gurion University of the Negev developed malware that could allow attackers to add realistic images of malignant tumours into CT or MRI scans before doctors had examined them. Worse still, they proved the same malware was able to remove real cancerous tumours from these images, which could lead to serious misdiagnosis and prevent patients receiving urgent critical care or surgery. Thankfully the group had developed this malware to highlight the need for improved cyber security in the healthcare sector, and had no intention of ever using it maliciously. And yet the existence of the research demonstrates the potential for attackers to seriously harm patients.

In 2019, The FDA provided recommendations concerning the potential exploitable vulnerabilities in radio frequency (RF) enabled St. Jude Medical implantable cardiac devices and the corresponding Merlin@home Transmitter. The FDA review of the St. Jude Medical's Merlin@home Transmitter confirmed should the vulnerabilities be exploited, an unauthorized user could remotely access a patient's RF-enabled implanted cardiac device by altering the Merlin@home Transmitter. The altered Merlin@home Transmitter could then be used to modify programming commands sent to the implanted device, which could result in rapid battery depletion and/or administration of inappropriate pacing or shocks. A validated software patch has been issued that will automatically update the Transmitter. The report states there have been no reports of patient harm resulting from these vulnerabilities.[3]

[2] Available: https://www.washingtonpost.com/local/medstar-health-turns-away-patientsone-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html. [Accessed 29 January 2017]. 12. ICS-CERT, "Hospira LifeCare PCA Infusion System Vulnerabilities (Update B)," 10 June 2015. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B. [Accessed 07 August 2016].

[3] FDA, "Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication," 09 January 2017. [Online]. Available: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm. [Accessed 23]

Critical data, end-to-end security

How is Philips leading the medical device cybersecurity effort?

Philips was an early leader in recognizing effective cybersecurity was no longer about protecting the 'box' or individual product, but a systematic approach that takes into account where and how devices are employed.

At Philips, 'Security Designed in' is an end-to-end mindset: infusing security principles begins with product design and development, through testing and deployment – and followed up with robust policies and procedures for monitoring, effective updates, and where necessary, incident response management. The organization chartered its own Product and Solutions Security Program to create, implement and update comprehensive and effective approaches to meet customer requirements and the Philips Security Center of Excellence shares information with leading cyber security researchers and test facilities around the world, assisting them to rapidly eliminate, reduce, and mitigate cyber threats.

With the company's focus on health technology, data privacy and security have become strategically vital, as health data is among the most sensitive types of personal data. In fact, the organization's competitive position relies heavily on the use of this data and public trust is paramount and its commitment to privacy goes far beyond regulatory compliance, with privacy and data protection controls embedded throughout the lifecycle of all data. Privacy and data protection are an integral part of the Philips General Business Principles, whereby we submit ourselves to a number of commitments.

January 2017]. 11. John Woodrow Cox, "MedStar Health turns away patients after likely ransomware cyberattack," The Washington Post, 29 March 2016. [Online].

Key Philips product security initiatives include:

Philips Product Security Policy
The Philips Product Security Policy is an industry-advanced, publicly available, consisting of policies, procedures, and standards empowering the organization to implement security best practices. It outlines the company's strategic organization and procedures for:

- Maintaining a global network of security and privacy professionals operating under the Philips Product Security Policy
- Developing and deploying best practices for our products and services
- Guiding risk assessment and incident response activities relating to potential and identified security and privacy threats and vulnerabilities
- Governing security embedded in product and services during their life-cycle, including risk assessment and response for identified vulnerabilities in products and services

Implementation of security standards that meet, or exceed, current regulatory requirements and industry best practices, including:

- Product security and privacy requirements for products and services which are not only aligned with the FDA-recommended standard ISO/IEC-800001, but were even used as the basis for the 80001-2-2 standard.
- Services security and privacy requirements aligned with recognized standards such as NIST 800-53 Rev 4, ITIL v3.1.24 and ISO/IEC-27000 series.
- Creation of customer-facing information such as the industry-standard Manufacturer Disclosure Statement for Medical Device Security (MDS2).
- Support for FDA guidance on Premarket Management on Cybersecurity in Medical Devices, and FDA Postmarket Management of Cybersecurity in Medical Devices.

Alignment with regulatory agencies, including the FDA

Philips is committed to the deployment of comprehensive security plans that assure the safety of medical devices, business enterprise information and personal data. And we do this within a heavily regulated medical device industry. Regulatory agencies such as the US Food and Drug Administration (FDA) require that hardware and software releases and changes be subjected to rigorous verification and validation methods to assure that high standards of safety, security, efficacy, quality and performance are met in all applicable Philips products and services.

FDA draft guidance: Content of premarket submissions for management of cybersecurity in medical devices (June 2013).

This draft guidance proposes that cybersecurity features be integrated into the device development phase and identifies information that should be incorporated into premarket submissions for medical devices. Security capabilities should cover three specific areas:

1. Limit access to trusted users only
2. Determine trusted content
3. Use fail safe and recovery features

Manufacturers should define and document the following:

- Identification of assets, threats, and vulnerabilities
- Impact assessment of the threats and vulnerabilities on device functionality • Assessment of the likelihood of a threat and of a vulnerability being exploited
- Determination of risk levels and suitable mitigation strategies
- Residual risk assessment and risk acceptance criteria

One insight from the guidance is the need for medical device manufacturers to produce evidence that their risk assessment process (as outlined in ISO 14971:2007) considered both “intentional” and unintentional security risks to the medical device and addressed those risks with appropriate security controls as part of the device’s design. The evidence should be included as part of the premarket approval submission package (e.g., 510K, PMA). Medical device manufacturers should consider during the early phases of the software life cycle the processes and actors (e.g., hackers, organized crime, terrorists, and nation states) that intentionally mean to compromise a medical device for the purpose of either a) harming the patient or b) extracting protected health information. Manufacturers also should consider collaborating with their customers’ clinical engineers and physicians to develop a catalog of use cases from which security vulnerabilities can be derived specific to their medical device and its intended use.

http://www.fda.gov/downloads/MedicalDevices/
DeviceRegulationandGuidance/GuidanceDocuments/ UCM356190.pdf

FDA safety communication: Cybersecurity for medical devices and hospital networks (June 2013).

This communication recommends that medical device manufacturers and health care facilities determine that appropriate safeguards are in place to reduce the risk of device failure due to a cyber-attack. Manufacturers are expected to take steps to limit unauthorized access to medical devices and to review policies and practices regarding appropriate safeguards. In keeping with the FDA communication, manufacturers should:

- Limit access to trusted users
- Protect individual components from exploitation
- Maintain a device’s critical functionality Health care facilities should:
  - Evaluate network security and protect the hospital system
  - Restrict unauthorized access to the network and networked medical devices
  - Determine that appropriate antivirus software and firewalls are up-to-date
  - Monitor network activity for unauthorized use
  - Protect individual network components through routine and periodic evaluation

http://www.fda.gov/MedicalDevices/Safety/ AlertsandNotices/ucm356423.htm

How to act now and safeguard medical devices?

With medical device cybersecurity threats, among the fastest growing risks for devices connected to private or public networks, regulators, including the US Food and Drug Administration (FDA) and the European Medicines Agency, now require medical device developers to include cybersecurity in risk management programmes for any device that could be connected to a network or another device, whether public or private, wired or wireless. (1, 2, 3)

Network connections potentially expose medical devices to threats from many sources – not just through a local router or server in a hospital or medical office, but from any computer, tablet, smart phone or even smart lightbulb connected to the Internet anywhere in the world. As a result regulators view cybersecurity as a shared responsibility.

Philips is committed to this risk sharing approach and provides extensive cybersecurity risk management strategies that incorporate input from all stakeholders. Through collaborating across the healthcare ecosystem, the industry can build on advances made by other critical infrastructure industries, supporting the advantages that digital connectivity will bring for patient care. “There is no one golden solution. Instead of it being a burden, we have to embrace security and privacy into our organizations,” says Michael McNeil, Head of Global Product & Security Services, Philips Healthcare. “Every one of us within this ecosystem needs to play our role in mitigating this threat.”

Cybersecurity risk management plans cover the entire life of the device, from development and testing throughout its use by healthcare professionals and/or with patients. They also address the wide range of potential threats, including deliberate or accidental disruption of device function, interference with data transfer between devices and servers, and any exposure of private medical data, or patient location or identity. And because hackers are highly inventive and persistent, our cybersecurity plans are continually and constantly updated, with probably current and future threats identified, monitored, and new mitigation strategies developed.

Five tips for improved medical device cybersecurity:

1. Have a clear overview
Clearly understand what products and assets are in your environment..

2. Focus on legacy products
Work with technology partners on any legacy types of products and solutions that might not have the capability to be updated, patched and secured.

3. Develop best practices
Make sure that you are working with an understanding of what are best practices from an industry perspective.

4. Work with manufacturers, vendors
It is important to work on your procurement processes and understand the components within the bill of materials of the solutions you provide.

5. Partner with manufacturers, vendors
Security – like safety and quality – is a prerequisite for confidence in the Philips brand. Customers and consumers must be able to rely on the security, safety and quality of our products and services and see the value of sharing their data – otherwise the health benefits that come from connectivity and analysis of big data sets may never be realized. To all senior leaders, you can be assured that we continue to be proactive in highlighting the benefits of connected health technology and continue to invest in secure systems that customers can rely on. Medical device cybersecurity is one of our growing centers of excellence, built on an understanding and appreciation of the interdependence of people, processes and technology.

Interested to learn more?

Let’s talk. Even better, let’s collaborate.

We’d love to help you apply Operational Intelligence to help solve your key people, process and technology challenges.

For more information, please visit [insert hub url]

How to reach us
Please visit www.philips.com
healthcare@philips.com