PHILIPS

Customer services

Customised service agreements designed to meet your evolving business needs

Our comprehensive Customer Service offer is adaptable to the specific needs of your organization. From maintenance, to IT, clinical capabilities and staff training, our services are designed to help you maximize your investments, make informed clinical decisions and keep your staff up to speed and motivated.

Connected Care service agreements

Benefits of having Philips as **your healthcare partner**

We create great services and deliver outcome-based solutions that are critical to your continuous success, through a deep understanding of your needs by **differentiating on technology, people and capabilities.**

Our commitment to you

- **Help you manage expenses through regular payments and optimise revenue**
  Enhance budget control with regular service payments and no unforeseen costs

- **Maximise system performance, protect your assets against cyber threats and drive compliance**
  Through software upgrades that provides the latest features and technology

- **Develop actionable insights and enhance productivity**
  Using patient monitoring data and workflows to make informed business decisions and improve your network management with PerformanceBridge Focal Point

- **Respond to your specific maintenance challenges**
  From first level support from our expert Philips engineers, to parts and proactive or corrective maintenance according to OEM standards

- **Extract the maximum value of your technology with our Philips Clinical Specialists**
  Clinical support at every stage of your technology journey delivered by our technology, people and capabilities

Software updates

Technology solutions

Clinical services

Phone and in person response

OEM spare parts

By teaming up with us to look after your systems, you can focus on what really matters – delivering better care, to more people, at lower costs.

Count on us, as your patients count on you.

The medical device cybersecurity imperative: high profile incidents have brought medical devices under scrutiny

> *"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

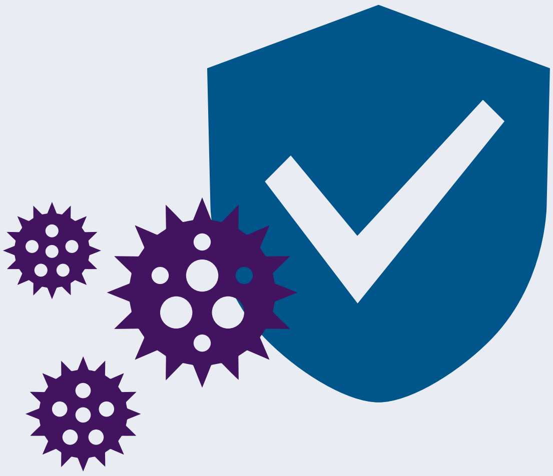
Several high profile incidents have brought medical device cybersecurity to the forefront of senior leader concerns. For example, the global ransomware event known as WannaCry – or the most recent ransomware attack on Health Service Executive – demonstrated how the performance of vulnerable medical devices 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 devices 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 protocol, 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
- 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

The medical device cybersecurity imperative: high profile incidents have brought medical devices under scrutiny

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 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 May 2021, the Irish Health Service was hit by a ransomware attack. The Health Service Executive (HSE), which is responsible for healthcare and social services across Ireland, was forced to shut down all its IT systems. HSE Director General Paul Reid said "there were 2,000 systems used by the health service and more than 4,500 servers" and the damage means tech specialists had to rebuild a "legacy network of 30 years". The number of appointments in some areas of the system has dropped by 80%.

"*https://www.rte.ie/newshealth/2021/0519/1222706-covid-hse/*" Speaking to RTÉ, the HSE's national clinical advisor Dr Vida Hamilton said it was "affecting every aspect of patient care". Dr Hamilton described the incident as a "major disaster" and said there were difficulties around accessing patient records. She said with lab tests, a handwritten form was required, with a runner taking it to the lab, and it then being manually put in to be analysed, something she said increased the chance of "delay and risk for error".
This attack on the HSE has been described as the most significant in the state's history and The HSE has said that 100 million euro would be a "small figure" in terms of the total cost of the cyberattack

Sources:
https://www.bbc.co.uk/news/world-europe-57154690
https://www.bbc.co.uk/news/world-europe-57184977
https://news.sky.com/story/callous-ransomware-attack-has-caused-catastrophic-damage-to-irish-health-care-system-12312243
https://www.belfasttelegraph.co.uk/news/republic-of-ireland/100-million-euro-would-be-small-figure-in-cost-of-hse-

Partnering to meet **your security needs**

You understand the importance of robust security, and consider it to be a critical concern. That's why we help you to identify, protect and monitor your systems, and support you in crisis situations.

✓ **RightFit Evolution:** future-proof your equipment with software maintenance

Maintaining software solutions

Helping you meet your **IT challenges**

✓ **Network assessment:** structured approach to assessing your patient monitoring network

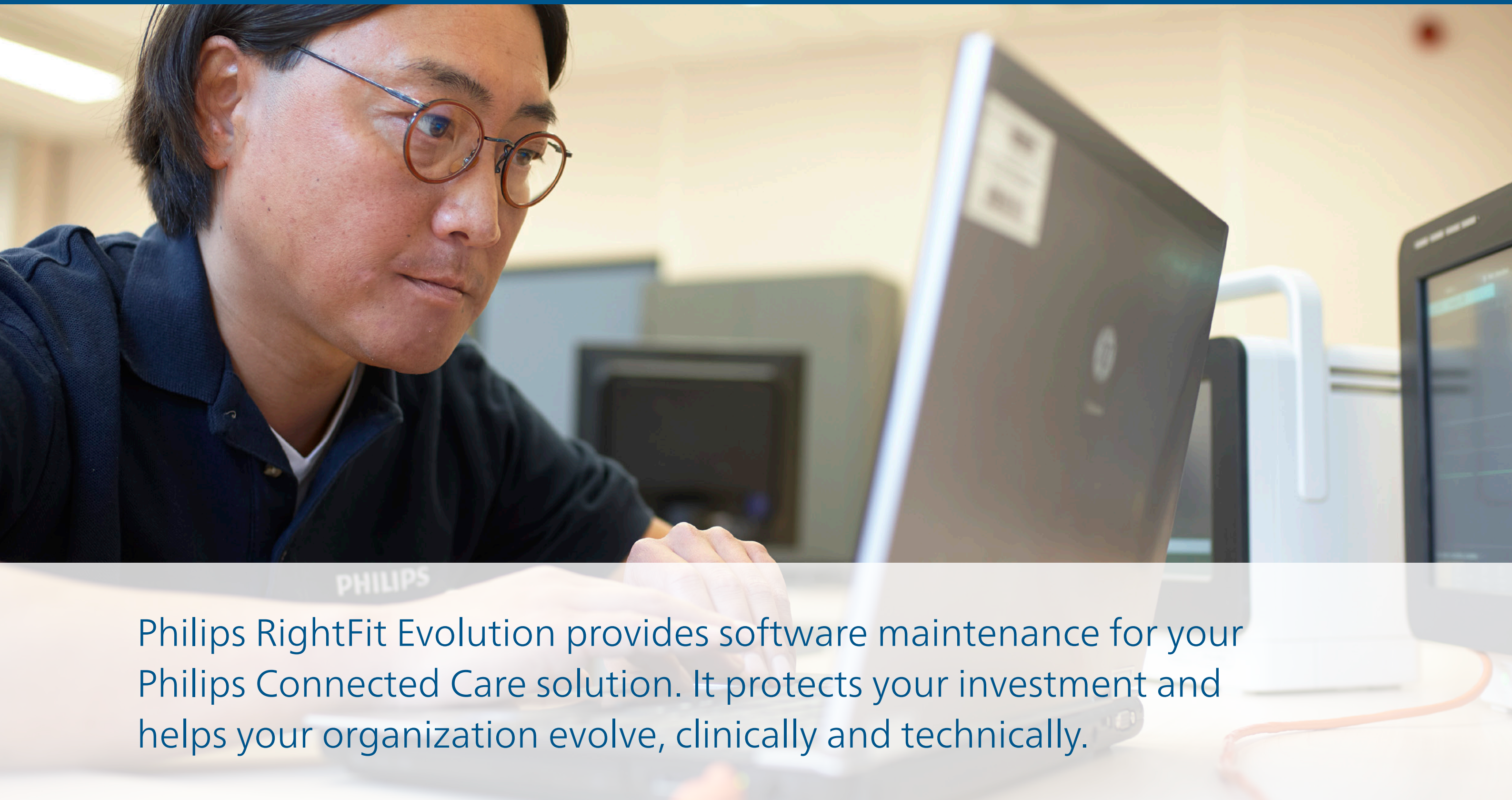
✓ **Performance Bridge Focal Point** for centralized operational management and strengthened security of Philips products

Delivering **remote security support**

Providing **physical security**

✓ **Philips OS patching:** central patch management for your Philips central stations

Keep your solutions up to date and secure **with RightFit Evolution**



Philips RightFit Evolution provides software maintenance for your Philips Connected Care solution. It protects your investment and helps your organization evolve, clinically and technically.

Software updates & fixes

- Regular software upgrades to ensure interoperability, compatibility and protection against cyber attacks for central stations and/or patient monitors
- RightFit Evolution includes unlimited access to software and enhancements, project management and implementation labour, and clinical go-live support and user training on new software revisions

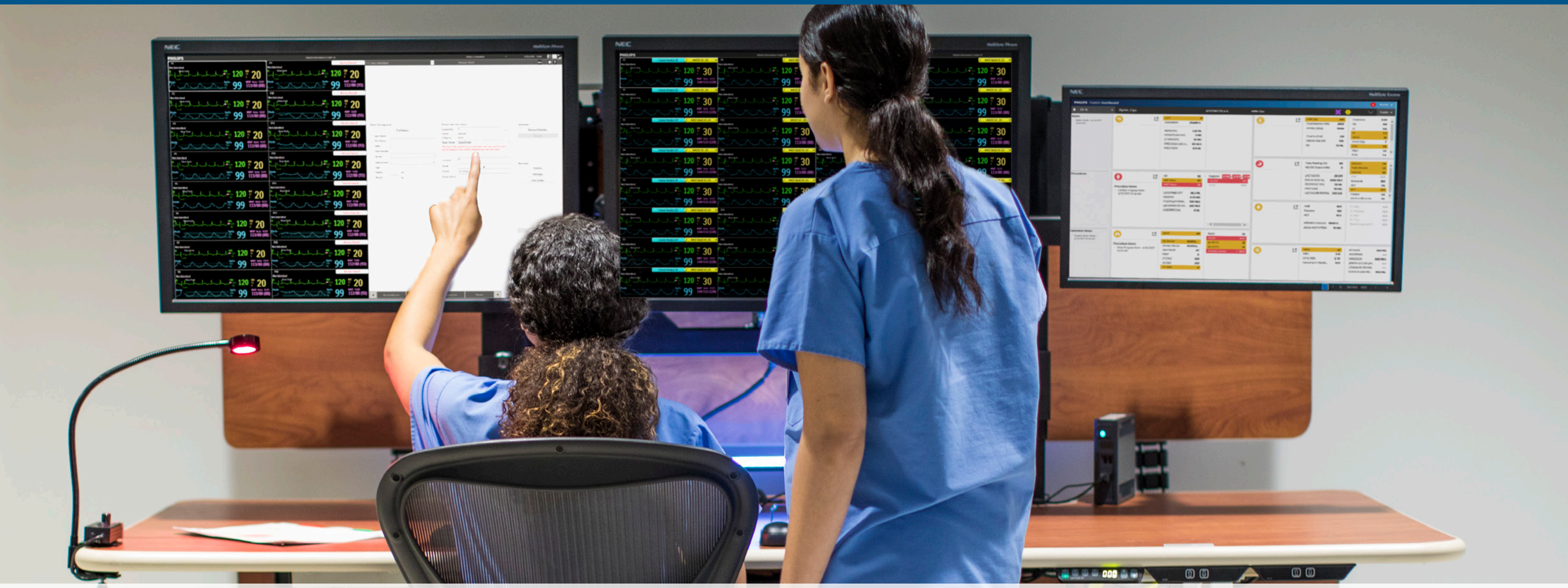
Consulting services

- Proactive communication and consulting on new software revisions, content, impact and requirements
- Project management and implementation support
- Clinical go-live support and user training on new software revisions

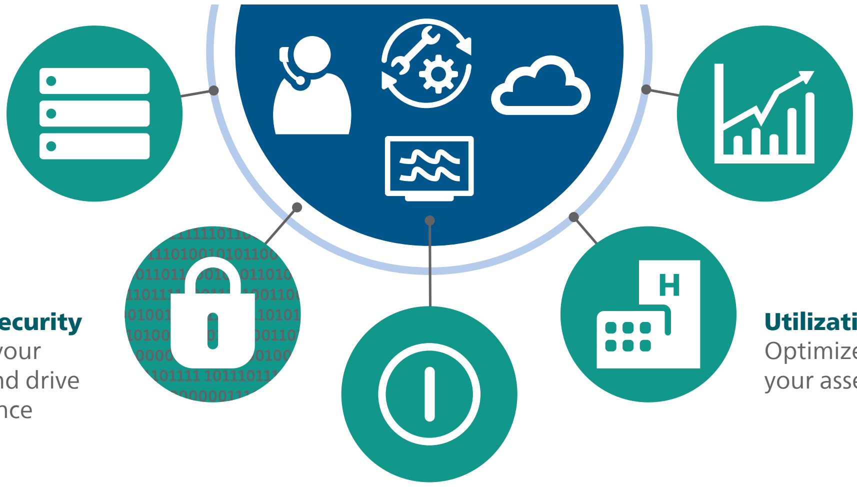
Hardware upgrade (optional)

- RightFit Evolution Advanced offers PC and/or server refresh when required by software upgrades

Optimize IT, business and clinical operations through **PerformanceBridge Focal Point**



By fostering the exchange of data and insights, PerformanceBridge Focal Point supports a proactive approach to optimisation, enhancing visibility, manageability and security of your devices, applications and network solutions.



Asset management
Know your assets: What/Where/ Status

Benchmarking & performance
Optimize your operations and clinical outcome

Cyber security
Protect your assets and drive compliance

Utilization
Optimize your assets

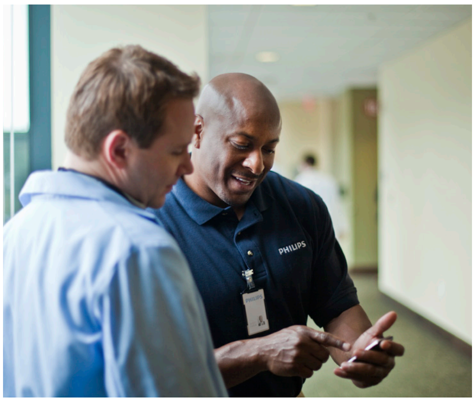
Availability
Ready when you need it where you need it

Philips OS patching service

- Controlled, semi-automated roll out of the latest security patches for the Microsoft™ operating system on PIC iX platform
- Central management of OS patches eases pressure to manually identify and install fixes
- Visibility and manageability of your devices, applications and network solution
- Patch can be handled by the customer (self-installation) or on-site by Philips

Complement your in-house capabilities and aim for zero downtime with **RightFit service agreements**

Pick and Mix amongst our RightFit portfolio to create your customised maintenance service agreements and meet your evolving business needs.



		Our team are so busy with corrective action but could do with support for annual servicing to remain compliant	*I only require ad-hoc support but would like financial predictability*	*We have an experienced team, however it would be great to have access to Philips experts and spend less time issuing POs for parts*	*I have too much on my plate and don't have time to look after my patient monitoring solution*
		Value	**Assist**	**Support**	**Primary**
		For those who most care about preventive maintenance	**Provides scalable coverage when you have in-house support**	**Provides OEM expertise and support for in-house biomeds teams**	**Delivers strong maintenance support with flexibility**
Parts and labour coverage	Labour and travel corrective maintenance	●	Bench labour only	Option	●
	Labour and travel preventive maintenance			Option	Option
	Normal parts		●	Option	●
	Software fixes	●	●	●	●
	Technical and application phone support		●	●	●
System availability	Initial telephone response *		1 hour	1 hour	1 hour
	Onsite response			Option next working day	Next working day
	Parts delivery time	Standard	Standard	Standard	Priority
	Technical remote services			●	●
Additional services	Remote / on-site clinical applications	●	●	Option	Option
	Consulting services			Option	Option

* Corrective and preventive maintenance service window: hours of coverage weekdays 9.00-17.00

To create and manage cases, view reports and contracts, please contact our support team at **customer.portal.uki@philips.com**

Keep your solutions up to date and secure **with RightFit Evolution**

The easiest and faster way to order your service parts:
Philips Healthcare Shop

Find what you need

- Part code & name validation to ensure you order the right product
- Real-time stock availability
- Order service parts under warranty and contract

Save time on reordering

- Bulk upload large orders
- Quick order functionality
- Fully responsive, use with any device 24/7

Make record-keeping simpler

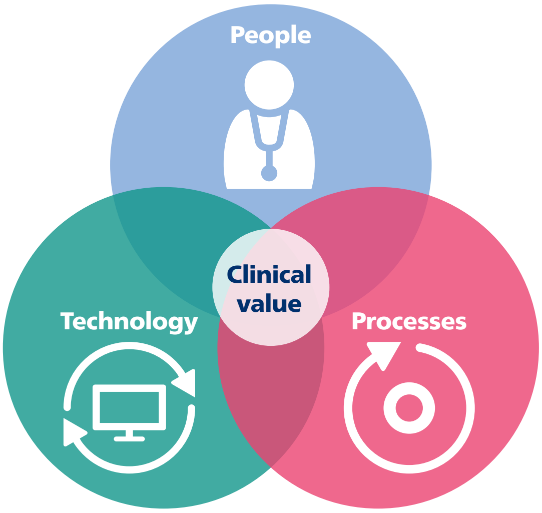
- View your contracted prices
- Track and trace your orders
- Search historical orders; both if they were made offline or online

Register today!

www.healthcare.shop.
Philips.co.uk/register

Connect with us
anywhere, anytime

Stay clinically advanced, maximize patient monitoring investments



From building a solid foundation of knowledge, to providing deep insights into a product or its features, to advanced utilization techniques, our clinical services experts will help you meet your objectives with their modular offering.

5 programs

Clinical Services Days
Clinical single days to deliver on clinical value with fully customized contend

Critical Care
Bundled Clinical Services for IntelliVue units, from the essential start, to the alarm management programs.

General Care
Bundle Services from essential spot check monitors training to workflow assessment

Upgrades
Specific programs when technology is upgraded and refreshers

Alarm notification
Support the implementation and change management needed to ensure the optimization of the Philips alarm notification solutions

Across 3 different levels

E^1 Essential

Effective use of systems
Training and education program to ensure safe handling of new Philips medical devices and encourage positive and committed workforce

E^2 Enhance

Make monitoring actionable and appropriate
Working together with you, we design a monitoring solution that complements your workflow and supports you to focus on your patients

E^3 Excel

Transform with technology
A clinically-focused program that evaluates your main current healthcare challenges and support implementation and change management initiatives

http://www.philips.co.uk