



PHILIPS


www.philips.com

Cybersecurity across the healthcare continuum

Ben Kokx

Director Product Security, Philips
Chair of the Cybersecurity focus group, COCIR

IHE Symposium – Rennes – 2019-04-09

innovation  you





Healthcare is increasingly depended on ICT



Systems are increasingly connected

A photograph of a hospital hallway. In the foreground, a woman in a white hospital gown is walking with a man in a blue sweater. The woman is holding a white device connected to wires. In the background, other hospital staff are visible. A teal banner is overlaid at the bottom of the image.

Systems are increasingly wireless



Systems become more 'intelligent'



Shift from products to services

The background image shows a busy operating room. Several surgeons in blue scrubs and masks are gathered around a patient on a table. In the foreground, a large Philips medical monitor displays multiple panels of data, including what appears to be a CT scan or similar imaging. The room is filled with various medical equipment, including IV stands and other monitors. A teal banner is overlaid at the bottom of the image.

Safety versus Security



The exchange of security information is essential

A control room with multiple computer monitors displaying data, with two people looking at the screens. The room has a grid wall and a window in the background. A woman is seated at a desk with several monitors, and a man in a white lab coat is standing next to her, looking at the screens. Another person is visible in the background, blurred. The text "Integration of networks and responsibilities?" is overlaid on a green banner at the bottom of the image.

Integration of networks and responsibilities?

A photograph of two men shaking hands in a hospital setting. The man on the left is wearing a white lab coat and is smiling. The man on the right is wearing a dark blue polo shirt with a name tag and is also smiling. They are standing in front of a piece of medical equipment, possibly a Philips X-ray machine. The background is a bright, clean hospital room.

Shared responsibility



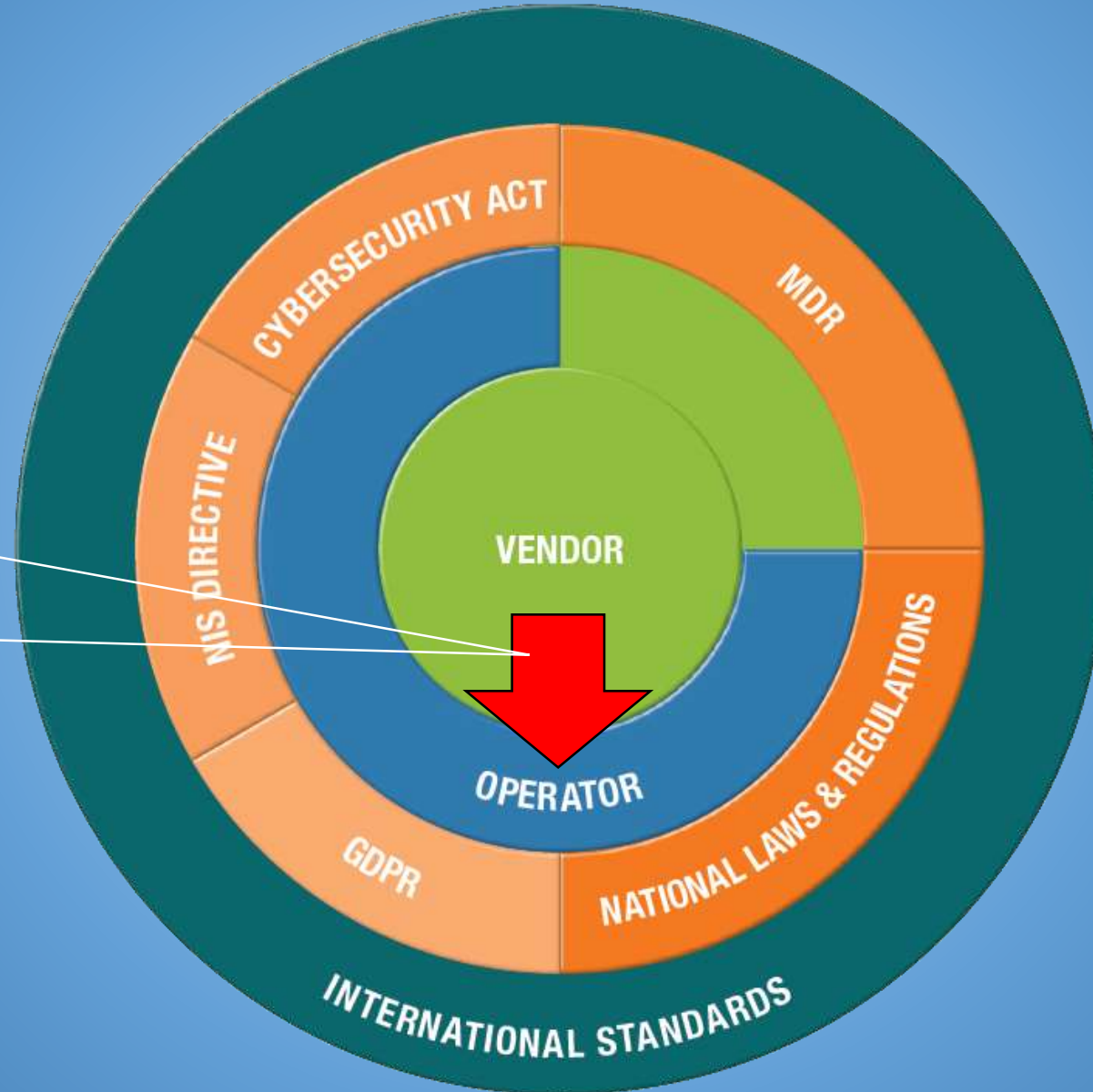
Digital revolution is also increasing risks



Do we manage on Risk or Compliance?

Compliance to which security requirements?

Define minimum requirements for the “intended environment”



Note: this is a simplified view, which does not show the entire complexity

To support secure healthcare in Europe, COCIR has developed the following recommendations for consideration by European, national and regional regulators:

1. **SET UP** a broad European discussion to establish good security practices in all regulatory frameworks, in order to reduce market access limitations, conflicting requirements and unnecessary administrative burden.
2. **PROMOTE** regulatory convergence between EU Member States and industry sectors.
3. **DEVELOP** European guidance that clarifies the concept of shared responsibility, including criteria for determining the device's intended environment.
4. **ADOPT** the new MDS2 form (currently under revision and expected to be adopted in Summer 2019) as a means of documenting and communicating medical device security and privacy features in Europe.
5. **COORDINATE** an European approach to security-related incident reporting, in order to avoid duplication and confusion.
6. **SAFEGUARD** a level playing field by ensuring that consistent and effective market surveillance measures are in place to warrant compliance with the existing regulatory framework.
7. **AVOID** multiple certification schemes for the same technologies and processes.



Examples of security related (Healthcare) standards that can be used in the life cycle of medical devices and health software

Pre-market process	Product Features	Documents	Post-market process
Establish secure development lifecycle	Build products with the appropriate security controls	Specify secure use	Security Management (updates and upgrades)
ISO/IEC 27034, IEC 62443-4-1, IEC 62304*, 82304, 80001-5-1*			
NIST FIPS 199 Security Categorization			
Threat/Risk Analysis ISO 14971* NIST SP800-30 IEC 62443-3-2* ISO 20004 ISO 27005 ISO 31000	IEC 60601-1 Safety EN 45502-1 & ISO 14708-1 Active implants ISO 22696 PHD Identification & Authentication IEC 60601-4-5 Safety related security spec* ISO 11633-1/2 Remote Service ISO 13606-4 EHR IHE IT Infrastructure Profiles NIST SP800-53 Security C ISO 15408 Common Crite	ISO 15026-1/2 Assurance case ISO 15443-1/2 Security assurance IEC 80001-2-2 IEC 80001-2-8 IEC 80001-2-9 HIMSS NEMA MDS2* CLSI AUTO-11-A2	ISO/IEC 29417 Disclosure ISO/IEC 30111 Vul./Incident ISO 270xx Information Security Management (Product operations)
ISO 270xx (Lifecycle) ISO 12207 ISO 15228 NIST SP800-160 SAFECODE OWASP MITRE CWE & CAPEC	ISO 18004 Timestamps ISO 18033 Encryption ISO 18367 Crypto algorithms ISO 18370 Digital Signatures ISO 19592 Secret Sharing ISO 19772 Auth. encryption ISO 27040 Secure Storage	NIST FIPS 140-2 Crypto Mod 180-4 Hashing 186-4 Digital Signatures 193 Platform Resilience 197 Encryption 198-1 Hash Msg Auth 200 Min Security Reqmts 201 Person Authentic 202 SHA-3	Black = Healthcare specific * = New or being revised

ISO/TC215 and IEC/TC62 development activities related to MDD/Health-IT security



Update ISO/IEC 80001-1(:2020-Q1)

Health informatics — Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software - Part 1: Application of risk management

NWIP ISO/IEC 80001-5-1(:2021-Q4)

Health informatics — Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software – Part 5: Security – Sub-Part 5-1: Activities in the Product Lifecycle

NWIP IEC TR 60601-4-5(:2020-Q2)

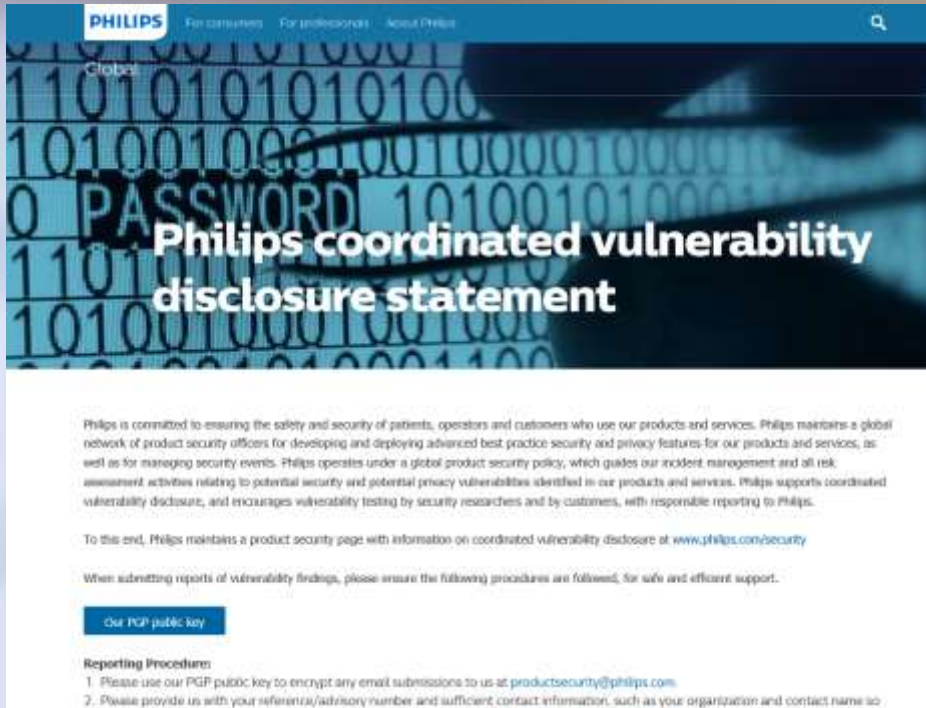
Medical electrical equipment – Part 4-5 Guidance and interpretation – Safety related technical security specifications for medical devices

NWIP ISO/IEC 81001-1(:2020-Q4)

Health informatics — Health software and health IT systems safety, effectiveness and security — Part 1: Foundational principles, concepts and terms

Update IEC 62304 ED2 (:2020-Q2)

Coordinated Vulnerability Disclosure

A screenshot of the Philips website's coordinated vulnerability disclosure statement. The page features a blue header with the Philips logo and navigation links for 'For consumers', 'For professionals', and 'About Philips'. The main content area has a background of binary code and a large 'PASSWORD' watermark. The title 'Philips coordinated vulnerability disclosure statement' is prominently displayed. Below the title, there is a paragraph of text explaining Philips's commitment to safety and security, followed by a link to their product security page. A section titled 'Reporting Procedure' lists two steps: using a PGP public key for encryption and providing reference/advisory numbers and contact information.

PHILIPS For consumers For professionals About Philips

Global

Philips coordinated vulnerability disclosure statement

Philips is committed to ensuring the safety and security of patients, operators and customers who use our products and services. Philips maintains a global network of product security officers for developing and deploying advanced best-practice security and privacy features for our products and services, as well as for managing security events. Philips operates under a global product security policy, which guides our incident management and all risk assessment activities relating to potential security and potential privacy vulnerabilities identified in our products and services. Philips supports coordinated vulnerability disclosure, and encourages vulnerability testing by security researchers and by customers, with responsible reporting to Philips.

To this end, Philips maintains a product security page with information on coordinated vulnerability disclosure at www.philips.com/security

When submitting reports of vulnerability findings, please ensure the following procedures are followed, for safe and efficient support.

[Our PGP public key](#)

Reporting Procedure:

1. Please use our PGP public key to encrypt any email submissions to us at productsecurity@philips.com.
2. Please provide us with your reference/advisory number and sufficient contact information, such as your organization and contact name so

ISO/IEC 29147; Vulnerability Disclosure

ISO/IEC 30111; Vulnerability Handling process



ADVANCING
CYBERSECURITY
OF HEALTH
AND **DIGITAL TECHNOLOGIES** MARCH 2019

COCIR SUSTAINABLE COMPETENCE IN ADVANCING HEALTHCARE

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry





Sustainable Competence
in Advancing Healthcare



Security



Fast response



In Control



Minimized risk



There are some
viruses doctors
can't treat.