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
Systems are increasingly wireless
Systems become more ‘intelligent’
Shift from products to services
Safety versus Security
The exchange of security information is essential
Integration of networks and responsibilities?
Shared responsibility
Digital revolution is also increasing risks
Do we manage on Risk or Compliance?
Define minimum requirements for the “intended environment”
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

<table>
<thead>
<tr>
<th>Pre-market process</th>
<th>Product Features</th>
<th>Documents</th>
<th>Post-market process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish secure development lifecycle</td>
<td>Build products with the appropriate security controls</td>
<td>Specify secure use</td>
<td>Security Management (updates and upgrades)</td>
</tr>
</tbody>
</table>

**ISO/IEC 27034, IEC 62443-4-1, IEC 62304*, 82304, 80001-5-1* |

**NIST FIPS 199 Security Categorization**

- 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 Controls
- ISO 15408 Common Criteria

- 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

**Threat/Risk Analysis**
- ISO 14971*
- NIST SP800-30
- IEC 62443-3-2*
- ISO 20004
- ISO 27005
- ISO 31000

**ISO 270xx (Lifecycle)**
- ISO 12207
- ISO 15228
- NIST SP800-160
- SAFECode
- OWASP
- MITRE CWE & CAPEC

**ISO 180xx**
- Timestamps
- Encryption
- Crypto algorithms
- Digital Signatures
- Secret Sharing
- Auth. encryption
- Secure Storage

**IEC 60601-4-5**
- Safety related security spec*

**ISO 15026**
- Assurance case

**ISO 15443-1/2**
- Security assurance

**ISO/IEC 29417 Disclosure**
- ISO/IEC 30111 Vul./Incident

**ISO 270xx Information Security Management**
- (Product operations)

**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

ISO/IEC 29147; Vulnerability Disclosure
ISO/IEC 30111; Vulnerability Handling process
There are some viruses doctors can’t treat.