IMDRF/DITTA Joint Virtual Workshop

12 September 2022

Health Software Standards – Security

Needs & Challenges

Varun Verma

Philips Healthcare / DITTA Cybersecurity WG Vice-Chair
Global Manager – Regulations & Standards at Philips Healthcare

• In the medical device industry for a little over 12 years in varying roles within R&D, engineering and global regulations and standards

• Current areas of focus include but are not limited to security and privacy in the healthcare field

Leadership role within DITTA:

• Vice-Chair of DITTA Cybersecurity Working Group

Expert Roles:

• In various national and international standards technical committees and working groups (ISO, IEC, AAMI), public private entities like HSCC, U.S. based trade associations including AdvaMed, MITA, HSCC, MDMA, CTA.
AGENDA

- Brief overview of security* related standards
- Considerations for developing healthcare related security standards
- Need for regulatory stakeholder collaboration
- Key challenges

* NOTE: Terms security and cybersecurity are used interchangeably.
<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>

### OVERVIEW OF SECURITY RELATED STANDARDS PUBLICATIONS

**ISO 27034, IEC 62443-4-1, IEC 62304*, IEC 82304-1, IEC 81001-5-1**

#### NIST FIPS 199 Security Categorization

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

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

**ISO**
- 18004 Timestamps
- 18033 Encryption
- 18367 Crypto algorithms
- 18370 Digital Signatures
- 19592 Secret Sharing
- 19772 Auth. encryption
- 27040 Secure Storage

**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

**ISO 15026-1/2**
- Assurance case

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

**IEC TR 80001-2-2***
- IEC TR 80001-2-8*
- IEC TR 80001-2-9
- HIMSS NEMA
- MDS2*
- CLSI AUTO-11-A2

---

* = New or being/planned to be revised

Black = Healthcare specific

ISO/IEC 29417 Disclosure
ISO/IEC 30111 Vul./Incident
ISO 270xx Information Security Management (Product operations)
CONSIDERATIONS FOR HEALTH SOFTWARE - SECURITY STANDARDS

Security requirements need to:

- Consider safety and performance
- Consider that security risk mitigation is a shared responsibility
- Be appropriate for the intended use and the environment of use
- Be appropriate for the technologies used
- Consider that existing and well accepted works can be adapted with little modification to the healthcare sector and health software
- Reflect that harm is harm regardless of the source of harm

There are many security standards developed by different TCs for specific purposes.
Collaboration among healthcare technology stakeholders adds tremendous value — regulators and health software developers have worked well together and can continue to work together.

**Harmonize conformity assessment through use of standards developed with conformity assessment in mind!**

- **Propose new work items!**

- **Regulators** have been involved with several valuable initiatives to the industry, but similar initiatives are encouraged to improve availability of state-of-the-art security standards globally.
- Timely recognition of standards
- Adoption with national deviations of existing international standards
- Harmonization of security standards in the EU

EU Standards strategy – common specifications

- Regulator stakeholder participation
Thank you!