

# ISO/IEEE 11073-40102:2022-03 (E)

## Health informatics - Device interoperability - Part 40102: Foundational - Cybersecurity - Capabilities for mitigation

---

### Contents

Page

- 1. Overview ..... 11
  - 1.1 General ..... 11
  - 1.2 Scope ..... 12
  - 1.3 Purpose ..... 12
  - 1.4 Word usage ..... 12
- 2. Normative references ..... 13
- 3. Definitions, acronyms, and abbreviations ..... 13
  - 3.1 Definitions ..... 13
  - 3.2 Acronyms and abbreviations ..... 13
- 4. Information security ..... 14
  - 4.1 General ..... 14
  - 4.2 Confidentiality ..... 14
  - 4.3 Integrity ..... 14
  - 4.4 Availability ..... 14
  - 4.5 Non-repudiation ..... 15
- 5. Security with safety and usability ..... 15
  - 5.1 High-level view ..... 15
  - 5.2 Safety relationships ..... 15
  - 5.3 Usability relationships ..... 16
- 6. Mitigation ..... 16
  - 6.1 General ..... 16
  - 6.2 Software security updates ..... 17
  - 6.3 Secure design principles ..... 17
  - 6.4 Secure by design and secure by default principles ..... 18
  - 6.5 Privacy by design and privacy by default principles ..... 18
  - 6.6 Ensure robust interface design ..... 19
  - 6.7 Limit access to trusted users only ..... 19
  - 6.8 Ensure trusted content ..... 19
  - 6.9 Mapping of mitigation categories, security capabilities, mitigation techniques, and design principles ..... 19
- 7. Information security controls ..... 22
- 8. Information security toolbox ..... 23
  - 8.1 General ..... 23
  - 8.2 Nonce ..... 24
  - 8.3 Encryption ..... 24
  - 8.4 Message authentication code ..... 24
  - 8.5 Key exchange ..... 25
  - 8.6 Key derivation function ..... 26
  - 8.7 Audit trail ..... 26
- Annex A (informative) Bibliography ..... 27
- Annex B (informative) Test vectors ..... 29
  - B.1 General ..... 29
  - B.2 NIST AES-GCM test vector ..... 29
  - B.3 NIST AES-GMAC test vector ..... 29
  - B.4 NIST ECDH test vectors ..... 30