IEC/TS 81001-2-2:2025-09 (E)

Health software and health IT systems safety, effectiveness and security - Part 2-2: Guidance for the implementation, disclosure and communication of security needs, risks and controls

Contents

Page

FOREWORD 3
INTRODUCTION 5
1 Scope 7
2 Normative references 8
3 Terms and definitions 8
4 Use of security capabilities 9
4.1 Structure of a *security capability* entry 9
4.2 Guidance on the communication of *security* capabilities and shared responsibility 9
4.3 Guidance for use of *security* capabilities in the *risk management process* 9
4.4 Guidance on the application of *risk management processes* 9
5 Security capabilities 10
5.1 General 10
5.2 Automatic logoff (ALOF) 11
5.3 Audit controls (AUDT) 11
5.4 Authorization (AUTH) 12
5.5 Cybersecurity product upgrades (CSUP) 13
5.6 Health data de-identification (DIDT) 14
5.7 Data backup and disaster recovery (DTBK) 15
5.8 Emergency access (EMRG) 15
5.9 Health data integrity and authenticity (IGAU) 16
5.10 Malware detection/protection (MLDP) 16
5.11 Node authentication (NAUT) 17
5.12 Person authentication (PAUT) 18
5.13 Physical locks on product (PLOK) 19
5.14 Third-party components in product life cycle roadmaps (RDMP) 19
5.15 System and application hardening (SAHD) 20
5.16 Health data storage confidentiality (STCF) 20
5.17 Transmission confidentiality (TXCF) 21
5.18 Transmission integrity and authenticity (TXIG) 21
6 Additional supporting information 21
6.1 General 21
6.2 Connectivity capabilities (CONN) 22
6.3 Management of personally identifiable information (MPII) 22
6.4 Remote services (RMOT) 23
6.5 Software Bill of Materials (SBOM) 24
6.6 *Security* guides (SGUD) 25
7 Examples of some *security* capabilities 25
7.1 Example of detailed specification under *security capability*: Person authentication (PAUT) 25

7.2 Example for Software Bill of Materials (SBOM) 26
8 References and other resources 27
8.1 General 27
8.2 *Manufacturer* disclosure statement for *medical device security* (MDS2) 28
8.3 Application *security* questionnaire (ASQ) 28
8.4 HL7 Functional Electronic Health Record (EHR) 28
8.5 Standards and frameworks 28
Annex A (informative) Sample scenario showing the exchange of security information 31
A.1 Introduction to the *security* characteristics scenario 31
A.2 Manufacturer Disclosure Statement for Medical device Security (MDS2) 32
Annex B (informative) Examples of regional specification on a few *security* capabilities 46
Annex C (informative) Guidance for selecting *security control*s to satisfy the *security* capabilities 49
C.1 General 49
C.2 Automatic logoff (ALOF) 52
C.3 Audit controls (AUDT) 53
C.4 Authorization (AUTH) 55
C.5 Cybersecurity product upgrades (CSUP) 58
C.6 Health data de-identification (DIDT) 59
C.7 Data backup and disaster recovery (DTBK) 61
C.8 Emergency access (EMRG) 63
C.9 Health data integrity and authenticity (IGAU) 64
C.10 Malware detection/protection (MLDP) 66
C.11 Node authentication (NAUT) 69
C.12 Person authentication (PAUT) 72
C.13 Physical locks on product (PLOK) 74
C.14 Third-party components in product life cycle roadmaps (RDMP) 76
C.15 System and application hardening (SAHD) 78
C.16 Health data storage confidentiality (STCF) 82
C.17 Transmission confidentiality (TXCF) 84
C.18 Transmission integrity and authenticity (TXIG) 86
C.19 Connectivity capabilities (CONN) 87
C.20 Management of personally identifiable information (MPII) 89
C.21 Remote services (RMOT) 90
C.22 Software Bill of Materials (SBOM) 92
C.23 Security guides (SGUD) 93
Annex D (informative) *Security capability* and additional *security* information mapping to C-I-A-A-A 97
Bibliography 99
Alphabetized index of defined terms 103

Figure 1 – *Health software* Field of Application as shown in IEC 81001-5-1 [3] 7
Figure 2 – Sample Structure for "*Medical device*2" 26

Table 1 – Example SBOM for "Medical device2" 27
Table D.1 – Sample mapping by a hypothetical *HDO* 97