

IEC/TR 80001-2-2:2012-07 (E)

Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the communication of medical device security needs, risks and controls

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	8
3 Terms and definitions	8
4 Use of SECURITY CAPABILITIES.....	12
4.1 Structure of a SECURITY CAPABILITY entry.....	12
4.2 Guidance for use of SECURITY CAPABILITIES in the RISK MANAGEMENT PROCESS	12
4.3 Relationship of ISO 14971-based RISK MANAGEMENT to IT security RISK MANAGEMENT.....	13
5 SECURITY CAPABILITIES	14
5.1 Automatic logoff – ALOF	14
5.2 Audit controls – AUDT	14
5.3 Authorization – AUTH.....	15
5.4 Configuration of security features – CNFS.....	16
5.5 Cyber security product upgrades – CSUP.....	16
5.6 HEALTH DATA de-identification – DIDT.....	17
5.7 Data backup and disaster recovery – DTBK.....	17
5.8 Emergency access – EMRG	17
5.9 HEALTH DATA integrity and authenticity – IGAU	18
5.10 Malware detection/protection – MLDP	18
5.11 Node authentication – NAUT	18
5.12 Person authentication – PAUT	19
5.13 Physical locks on device – PLOK	19
5.14 Third-party components in product lifecycle roadmaps – RDMP	20
5.15 System and application hardening – SAHD.....	20
5.16 Security guides – SGUD.....	21
5.17 HEALTH DATA storage confidentiality – STCF	21
5.18 Transmission confidentiality – TXCF.....	22
5.19 Transmission integrity – TXIG	22
6 Example of detailed specification under SECURITY CAPABILITY: Person authentication – PAUT.....	22
7 References.....	23
8 Other resources.....	25
8.1 General.....	25
8.2 Manufacture disclosure statement for medical device security (MDS2)	25
8.3 Application security questionnaire (ASQ).....	25
8.4 The Certification Commission for Healthcare Information Technology (CCHIT).....	25
8.5 http://www.cchit.org/get_certified HL7 Functional Electronic Health Record (EHR).....	26
8.6 Common criteria – ISO/IEC 15408.....	26

9 Standards and frameworks	26
Annex A (informative) Sample scenario showing the exchange of security information.....	27
Annex B (informative) Examples of regional specification on a few SECURITY CAPABILITIES	48
Annex C (informative) SECURITY CAPABILITY mapping to C-I-A-A	52
Bibliography	53
Table 1 – Relationship of IT security and ISO 14971-based terminology	13
Table C.1 – Sample mapping by a hypothetical HDO	52