

IEC/TR 80001-2-8:2016-05 (E)

Application of risk management for IT-networks incorporating medical devices - Part 2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	9
2 Normative references.....	9
3 Terms and definitions	10
4 Guidance for establishing SECURITY CAPABILITIES	13
4.1 General.....	13
4.2 Automatic logoff – ALOF	14
4.3 Audit controls – AUDT	15
4.4 Authorization – AUTH.....	17
4.5 Configuration of security features – CNFS	19
4.6 Cyber security product upgrades – CSUP	21
4.7 HEALTH DATA de-identification – DDT	24
4.8 Data backup and disaster recovery – DTBK	25
4.9 Emergency access – EMRG	27
4.10 HEALTH DATA integrity and authenticity – IGAU	28
4.11 Malware detection/protection – MLDP	30
4.12 Node authentication – NAUT	32
4.13 Person authentication – PAUT	35
4.14 Physical locks on device – PLOK.....	37
4.15 Third-party components in product lifecycle roadmaps – RDMP.....	39
4.16 System and application hardening – SAHD	42
4.17 Security guides – SGUD	44
4.18 HEALTH DATA storage confidentiality – STCF	47
4.19 Transmission confidentiality – TXCF	48
4.20 Transmission integrity – TXIG.....	50
Bibliography	51

Table 1 – ALOF controls	14
Table 2 – AUDT controls	16
Table 3 – AUTH controls	18
Table 4 – CNFS controls	20
Table 5 – CSUP controls	22
Table 6 – DIDT controls	24
Table 7 – DTBK controls	26
Table 8 – EMRG controls	28
Table 9 – IGAU controls	29
Table 10 – MLDP controls	30
Table 11 – NAUT controls	33
Table 12 – PAUT controls	36
Table 13 – PLOK controls	38
Table 14 – RDMP controls	40
Table 15 – SAHD controls	43
Table 16 – SGUD controls	45
Table 17 – STCF controls	48
Table 18 – TXCF controls	49
Table 19 – TXIG controls	50