ISO/TS 6268-3:2026-10 (E)

Health informatics - Cybersecurity framework for telehealth environments - Part 3: Cybersecurity controls of telehealth

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms,definitionsandabbreviatedterms 1
3.1 Terms and definitions 1
3.2 Abbreviated terms 2

4 Cybersecurity controls for telehealth services 2
4.1 General 2
4.2 Organizational controls 3
4.2.1 Cybersecurity alignment and gap management 3
4.2.2 Contact with authorities and support systems 3
4.2.3 Asset identification and management 4
4.2.4 Cybersecurity level alignment 5
4.2.5 Secure exchange of telehealth information 5
4.2.6 Shared identity management 6
4.2.7 Telehealth incident management planning and preparation 7
4.2.8 Differences in legal, statutory, regulatory and contractual requirements 7
4.2.9 Protection of records 8
4.2.10 Documented operating procedures 8
4.2.11 Unique identification and authentication 9
4.3 People controls 10
4.3.1 Identification of participating persons 10
4.3.2 Awareness, education and training for persons participating in telehealth services 10
4.3.3 Social engineering 11
4.4 Physical controls 12
4.4.1 Physical security perimeters 12
4.4.2 Telehealth services in private non-clinical spaces 13
4.4.3 Protecting real-time services against physical and environmental threats 13
4.4.4 Telehealth equipment management 14
4.5 Technological controls 15
4.5.1 Personally-managed telehealth devices 15
4.5.2 Authentication of authorized patient assistants 15
4.5.3 Home monitoring devices in telehealth environments 16
4.5.4 Configuration for critical telehealth services 17

Annex A (informative) Alignment of telehealth cybersecurity controls with ISO 27799:2025 18

Bibliography 20