ISO/TS 25237:2008-12 (E)

Health informatics - Pseudonymization

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols (and abbreviated terms) 6

5 Requirements for privacy protection of identities in healthcare 6
5.1 A conceptual model for pseudonymization of personal data 6
5.2 Categories of data subject 13
5.3 Classification of data 14
5.4 Trusted services 16
5.5 Need for re-identification of pseudonymized data 16
5.6 Pseudonymization service characteristics 17

6 Pseudonymization process (methods and implementation) 18
6.1 Design criteria 18
6.2 Entities in the model 18
6.3 Workflow in the model 20
6.4 Preparation of data 21
6.5 Processing steps in the workflow 22
6.6 Protecting privacy protection through pseudonymization 23

7 Re-identification process (methods and implementation) 27

8 Specification of interoperability of interfaces (methods and implementation) 28

9 Policy framework for operation of pseudonymization services (methods and implementation) 29
9.1 General 29
9.2 Privacy policy 29
9.3 Trustworthy practices for operations 30
9.4 Implementation of trustworthy practices for re-identification 31

Annex A (informative) Healthcare pseudonymization scenarios 33

Annex B (informative) Requirements for privacy risk assessment design 46

Bibliography 56