

ISO 25237:2017-01 (E)

Health informatics - Pseudonymization

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	6
5	Requirements for privacy protection of identities in healthcare	7
5.1	Objectives of privacy protection	7
5.2	General	7
5.3	De-identification as a process to reduce risk	8
5.3.1	General	8
5.3.2	Pseudonymization	8
5.3.3	Anonymization	9
5.3.4	Direct and indirect identifiers	9
5.4	Privacy protection of entities	9
5.4.1	Personal data versus de-identified data	9
5.4.2	Concept of pseudonymization	11
5.5	Real world pseudonymization	13
5.5.1	Rationale	13
5.5.2	Levels of assurance of privacy protection	14
5.6	Categories of data subject	16
5.6.1	General	16
5.6.2	Subject of care	16
5.6.3	Health professionals and organizations	16
5.6.4	Device data	16
5.7	Classification data	17
5.7.1	Payload data	17
5.7.2	Observational data	17
5.7.3	Pseudonymized data	17
5.7.4	Anonymized data	17
5.8	Research data	17
5.8.1	General	17
5.8.2	Generation of research data	18
5.8.3	Secondary use of personal health information	18
5.9	Identifying data	18
5.9.1	General	18
5.9.2	Healthcare identifiers	18
5.10	Data of victims of violence and publicly known persons	19
5.10.1	General	19
5.10.2	Genetic information	19
5.10.3	Trusted service	19
5.10.4	Need for re-identification of pseudonymized data	19
5.10.5	Pseudonymization service characteristics	20
6	Protecting privacy through pseudonymization	20
6.1	Conceptual model of the problem areas	20

6.2	Direct and indirect identifiability of personal information	21
6.2.1	General	21
6.2.2	Person identifying variables	21
6.2.3	Aggregation variables	21
6.2.4	Outlier variables	22
6.2.5	Structured data variables	22
6.2.6	Non-structured data variables	23
6.2.7	Inference risk assessment	23
6.2.8	Privacy and security	24
7	Re-identification process	24
7.1	General	24
7.2	Part of normal procedures	24
7.3	Exception	24
7.4	Technical feasibility	25
Annex A (informative) Healthcare pseudonymization scenarios		26
Annex B (informative) Requirements for privacy risk analysis		39
Annex C (informative) Pseudonymization process (methods and implementation)		49
Annex D (informative) Specification of methods and implementation		55
Annex E (informative) Policy framework for operation of pseudonymization services (methods and implementation)		56
Annex F (informative) Genetic information		60
Bibliography		61