

ISO 22857:2004-04 (E)

Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health information

Contents		Page
Foreword		vii
Introduction		ix
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	3
5	Structure of this International Standard	3
6	General principles and roles	3
6.1	General principles	3
6.2	Roles	4
7	Legitimising data transfer	4
7.1	The concept of "adequate" data protection	4
7.2	Conditions for legitimate transfer	5
8	Criteria for ensuring adequate data protection with respect to the transfer of personal health data	6
8.1	The requirement for adequate data protection	6
8.2	Content principles	6
8.3	Procedural/enforcement mechanisms	8
8.4	Contracts	10
8.5	Overriding laws	10
8.6	Anonymisation	11
8.7	Legitimacy of Consent	11
9	Security policy	12
9.1	General	12
9.2	The purpose of the security policy	12
9.3	The "level" of security policy	12
9.4	High Level Security Policy: general aspects	13
10	High Level Security Policy: the content	14
10.1	Principle One: overriding generic principle	14
10.2	Principle Two: chief executive support	15
10.3	Principle Three: documentation of Measures and review	15
10.4	Principle Four: Data Protection Security Officer	16
10.5	Principle Five: permission to process	16
10.6	Principle Six: information about processing	17
10.7	Principle Seven: information for the data subject	19
10.8	Principle Eight: prohibition of onward data transfer without consent	19
10.9	Principle Nine: remedies and compensation	20
10.10	Principle Ten: security of processing	21
10.11	Principle Eleven: responsibilities of staff and other contractors	22

11	Rationale and Observations on Measures to support Principle Ten concerning security of processing	23
11.1	General	23
11.2	Encryption and digital signatures for transmission to the data importer	23
11.3	Access controls and user authentication	23
11.4	Audit trails	23
11.5	Physical and environmental security	24
11.6	Application management and network management	24
11.7	Malicious software	24
11.8	Breaches of security	24
11.9	Business Continuity Plan	24
11.10	Handling very sensitive data	24
11.11	Standards	25
12	Personal health data in non-electronic form	25
	Annex A (informative) Key primary international documents on data protection	26
	Annex B (informative) National documented requirements and legal provisions in a range of countries	32
	Annex C (informative) Relevant ISO and CEN Standards	35
	Annex D (informative) Sources of advice	36
	Annex E (informative) Exemplar contract clauses: Controller to Controller	38
	Annex F (informative) Exemplar contract clauses: Controller to Processor	47
	Annex G (informative) Handling very sensitive personal health data	57
	Bibliography	59