

# ISO 22857:2013-12 (E)

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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
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 .....	9
8.4	Contracts .....	10
8.5	Overriding laws .....	11
8.6	Anonymisation .....	11
8.7	Legitimacy of consent .....	12
9	Security policy .....	12
9.1	General .....	12
9.2	The purpose of the security policy .....	12
9.3	The "level" of security policy .....	13
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 .....	16
10.4	Principle Four: Data protection security officer .....	16
10.5	Principle Five: permission to process .....	17
10.6	Principle Six: information about processing .....	18
10.7	Principle Seven: information for the data subject .....	20
10.8	Principle Eight: prohibition of onward data transfer without consent .....	20
10.9	Principle Nine: remedies and compensation .....	21
10.10	Principle Ten: security of processing .....	22
10.11	Principle Eleven: responsibilities of staff and other contractors .....	23

<b>11</b>	<b>Rationale and observations on measures to support Principle Ten concerning security of processing .....</b>	<b>24</b>
<b>11.1</b>	<b>General .....</b>	<b>24</b>
<b>11.2</b>	<b>Encryption and digital signatures for transmission to the data importer .....</b>	<b>24</b>
<b>11.3</b>	<b>Access controls and user authentication .....</b>	<b>24</b>
<b>11.4</b>	<b>Audit trails .....</b>	<b>25</b>
<b>11.5</b>	<b>Physical and environmental security .....</b>	<b>25</b>
<b>11.6</b>	<b>Application management and network management .....</b>	<b>25</b>
<b>11.7</b>	<b>Malicious software .....</b>	<b>25</b>
<b>11.8</b>	<b>Breaches of security .....</b>	<b>25</b>
<b>11.9</b>	<b>Business continuity plan .....</b>	<b>25</b>
<b>11.10</b>	<b>Handling very sensitive data .....</b>	<b>26</b>
<b>11.11</b>	<b>Standards .....</b>	<b>26</b>
<b>12</b>	<b>Personal health data in non-electronic form .....</b>	<b>26</b>
	<b>Annex A (informative) Key primary international documents on data protection .....</b>	<b>27</b>
	<b>Annex B (informative) National documented requirements and legal provisions in a range of countries .....</b>	<b>32</b>
	<b>Annex C (informative) Exemplar contract clauses: Controller to controller .....</b>	<b>37</b>
	<b>Annex D (informative) Exemplar contract clauses: Controller to processor .....</b>	<b>44</b>
	<b>Annex E (informative) Handling very sensitive personal health data .....</b>	<b>53</b>
	<b>Bibliography .....</b>	<b>55</b>