

DIN EN ISO 20737:2026-11 (E)

Health informatics - Interoperability of personal health decision support services (ISO 20737:2026); English version EN ISO 20737:2026

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 Personal health decision support	3
5.1 General	3
5.2 Concept model	4
5.3 Data flows	4
5.3.1 General	4
5.3.2 Data flow between the PHDS service and data provider	5
5.3.3 Data flow between the PHDS service and PHDS client	6
5.4 Use cases	6
5.4.1 General	6
5.4.2 Deciding on a course of treatment	6
5.4.3 Managing a chronic disease	6
5.4.4 Understanding health risks	6
5.4.5 Adhering to a treatment plan	7
5.4.6 Choosing a healthcare provider	7
6 Interoperability requirements for personal health decision support	7
6.1 PHDS service	7
6.1.1 General	7
6.1.2 Support for health data exchange	7
6.1.3 Data acquisition via standardized APIs	7
6.1.4 Integration with PHDS clients	7
6.1.5 Validation of incoming health data	7
6.1.6 Automatic data synchronization	7
6.1.7 Semantic data mapping and transformation	7
6.1.8 Acknowledgement and error response generation	7
6.1.9 Robust error-handling mechanisms	8
6.1.10 Audit logging of data transactions	8
6.1.11 Transformation into decision-support-ready formats	8
6.1.12 Data visualization and reporting tools	8
6.2 Data provider	8
6.2.1 General	8
6.2.2 Use of standard data formats and terminologies	8
6.2.3 Secure transmission of health data	8
6.2.4 Support for updates and corrections	8
6.2.5 Metadata and provenance information	8
6.2.6 Real-time or near real-time data transmission	8
6.2.7 Consent-based data sharing	8
6.2.8 Multi-endpoint transmission support	9
6.2.9 Data compression	9
6.3 PHDS client	9
6.3.1 General	9

6.3.2	Result reception.....	9
6.3.3	Acknowledgement to PHDS service.....	9
6.3.4	Secure communication channel.....	9
6.3.5	User authentication and authorization	9
6.3.6	User-friendly result presentation.....	9
6.3.7	Customizable result display.....	9
6.4	Privacy and security considerations	9
6.4.1	General.....	9
6.4.2	Data encryption.....	10
6.4.3	Access control	10
6.4.4	Data retention	10
6.4.5	Incident response	10
6.4.6	Consent management.....	10
6.4.7	User-initiated data deletion.....	10
6.4.8	Security notifications.....	10
Bibliography.....		11