Compliance Preparation Plan for Healthcare Application (HA)

Version: 1.0

March 3th, 2022

Andersen Site

Contents

Contents

Contents

Terms and Definitions

Digital Health Application (DiGA):

- DiGA (Digitale Gesundheitsanwendung, Digital Health Applications) is a CE-marked (certified) medical device of Class I or IIa that performs its designated function via digital technologies and is used either by the patient or both the patient and the healthcare provider.

- DiGA is not a digital application only aimed at collecting data from a device or controlling it.

- DiGA supports the recognition, monitoring, treatment, or alleviation of diseases or the recognition, treatment, alleviation, or compensation of injuries or disabilities.

- DiGA is not used for primary prevention.

- DiGA is only used by the patient or by both the patient and the healthcare provider. This means that apps that are only used by the physician to treat patients (practice equipment) are not DiGA. DiGA is therefore a digital assistant for patients.

Medical Device Software (MDSW):

MDSW is software that is intended to be used, alone or in combination, for a purpose specified in the definition of a “medical device” in the Medical Device Regulation or the In Vitro Diagnostic Medical Device Regulation.

BfArM – the Federal Institute for Drugs and Medical Devices.

SGB V – (German) Social Code Book V.

Key Requirements to Achieve Compliance of HA with DiGA

- DiGAV (Digital Health Applications Ordinance) – Ordinance on the procedure and requirements for assessing the reimbursability of digital health apps in statutory health insurance;

- The Fast-Track Process for DiGA according to Section 139e SGB V. A Guide for Manufacturers, Service Providers and Users;

- DVG – (Digitale-Versorgung-Gesetz, The Digital Healthcare Act).

DVG came into effect on December 19th, 2019, introducing the “app on prescription” as part of healthcare provided to patients. This means that around 73 million insured by the statutory health insurance (Gesetzliche Krankenversicherung, GKV) are entitled to healthcare via DiGA. These apps can be prescribed by physicians and psychotherapists and are reimbursed by health insurers. Insured persons that can provide their GKV funds with proof of a corresponding indication are also eligible to receive the desired DiGA without a prescription.

The prerequisite for the above is that DiGA must successfully pass the assessment by BfArM, leading to a listing in a directory of reimbursable digital health applications (DiGA directory, hereinafter referred to as ‘directory’). The procedure is designed as a fast-track process: BfArM is expected to assess each DiGA within three months. The essence of this assessment is to examine the manufacturer’s statements about the product qualities – from data protection to user-friendliness – and to examine the evidence of its positive healthcare effect **(Figure 1 gives an overview of the procedure)**.

Key Requirements to Achieve Compliance of HA with DiGA

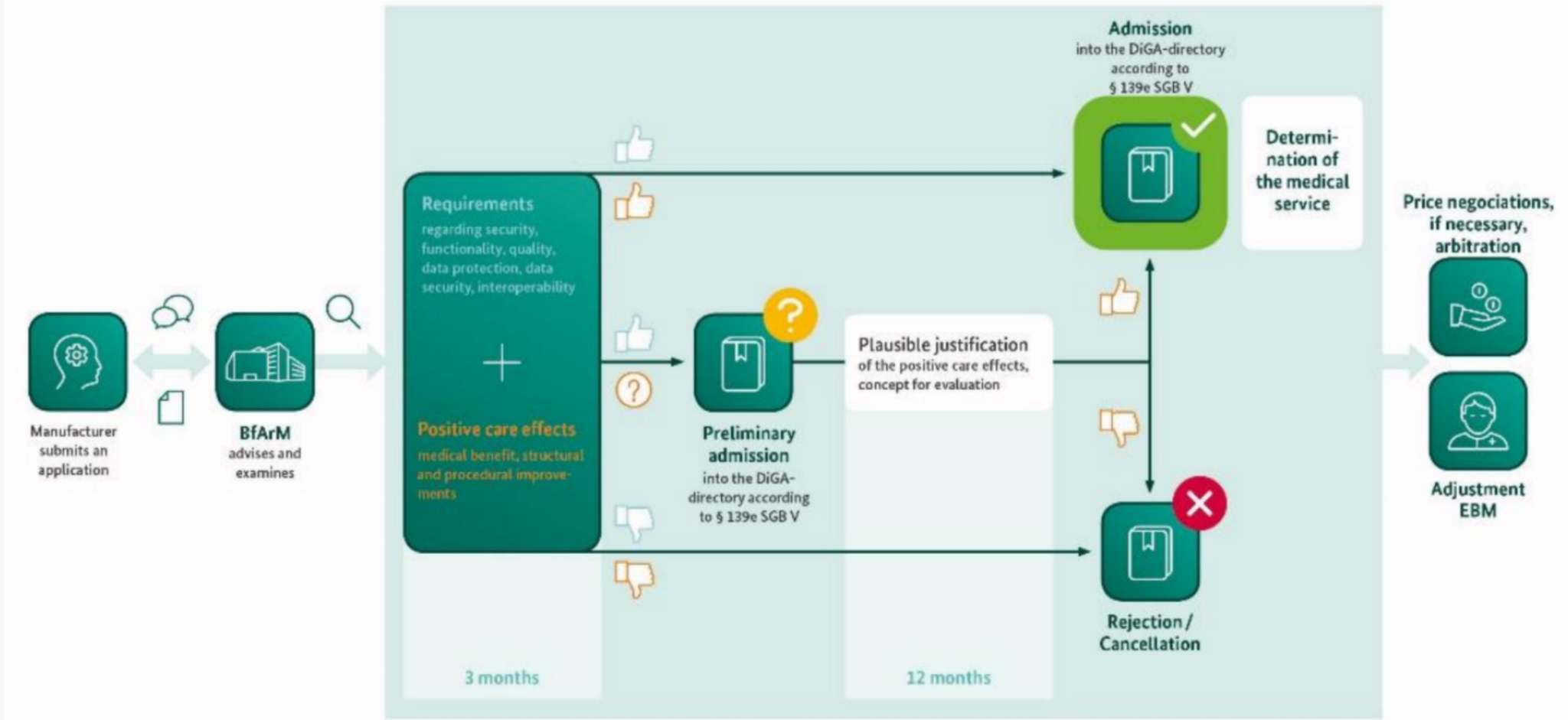

Figure 1 – Sequence of the Fast-Track procedure steps. Source: BfArM.

The Federal Ministry of Health (Bundesministerium für Gesundheit, BMG) has regulated the details of the application procedure, the requirements for DiGA, and the shape of the directory in DiGAV.

DiGAV is applicable for placing DiGA on the market in Germany. For this purpose, the application needs to comply with German legislation.

3.1 Qualification

- The Fast-Track Process for Digital Health Applications (DiGA) according to Section 139e SGB V. A Guide for Manufacturers, Service Providers and Users;

- The EU MDR 2017/745 is a Regulation of the European Parliament and of the Council of 5 April 2017 on medical devices.

HA is a digital app for children with a risk of developmental delay, which is aimed at:

- detecting, tracking, and alleviating developmental disabilities;

- tracking and interpreting a child's body temperature to enhance the detection of conditions associated with fever and changes in body temperature (upper respiratory infections, bacterial infections, endocrine disorders, etc.).

It should be noted that a change in or the addition of functionality to software may lead to its qualification as MDSW or a classification revision of this MDSW.

Similarly, a module added to software might be qualified as MDSW on its own.

MDSW of a higher Class (IIb, III) can't apply for the Fast-Track Process for DiGA.

Software module	DiGA's intended purpose
Authorization module	—
Settings	—
Profile (child)	—
Health records	✓
Smart devices	—
Notifications	✓
Onboarding	✓
Community support	—

*** Note:** Since this document is an example, the list of features is omitted. Usually, each feature is assessed.

3.2 Classification

- MDR – Article 51 – Classification of devices;
- MDR – Annex VIII – Classification rules;
- The Fast-Track Process for Digital Health Applications (DiGA) according to Section 139e SGB V. A Guide for Manufacturers, Service Providers and Users.

All DiGA must comply with the requirement to be a medical device of the risk Class I or IIa according to MDR.

Qualification and Classification

The risk class depends on the description of the conditions of use and clinical benefit. The medical purpose of the software medical device is determined by what the manufacturer indicates on the label of the device, instructions, and advertisements.

All implementing rules in Annex VIII to Regulation (EU) 2017/745 must be considered.

Rule	Explanation
The first sentence of the implementing **rule 3.3** of Annex VIII clarifies the regulations applicable to software driving or influencing the use of a device: “Software, which drives or influences the use of a device, shall fall within the same class as the device.”	HA is a health management system. HA will not drive or influence the use of a device.
Implementing **rule 3.5** of Annex VIII is relevant for all devices and states that: “If several rules, or if, within the same rule, several sub-rules, apply to the same device based on the device’s intended purpose, the strictest rule and sub-rule resulting in the higher classification shall apply.”	Rule 11 has been applied to classify PHI.
Rules 9, 10, and 12 mainly categorize the risks related to the exchange of energy/substances between the body and diagnostic or therapeutic active devices, taking into account the different healthcare situations (conditions of patients).	HA is a health management system. HA does not contain any risks related to the exchange of energy/substances between the body and diagnostic or therapeutic active devices.
Rule 11 – Software for decisions with diagnosis or therapeutic purposes or software intended to monitor physiological processes.	Rule 11 has been applied to classify HA.
Software intended to provide information that is used to make decisions with diagnosis or therapeutic purposes is classified as Class IIa, except when such decisions have an impact that may cause: • death or an irreversible deterioration of a patient's state of health – in this case, it is Class III; • a serious deterioration of a patient's state of health or surgical intervention – in this case, it is Class IIb.	HA is intended to provide information that is used to make decisions for therapeutic purposes.

Qualification and Classification

Software intended to monitor physiological processes belongs to Class IIa, except when it is intended to monitor vital physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient – in this case, it is Class IIb.	HA is not intended to monitor physiological processes.
All other software belongs to Class I.	HA belongs to Class I.

MDSW/DiGA	Rule	Class
HA	11	I

Since HA is a medical device of Class I according to MDR, the Fast-Track Process for Digital Health Applications (DiGA), according to Section 139e SGB V, can be applied to expedite the entry of the product to the German marketplace.

4.1 Introduction

- MDR – Article 10 – General obligations of manufacturers;
- ISO 13485 Medical devices – Quality management systems;
- CEN/TR 17223 – describes how to combine ISO 13485 and MDR Article 10;
- IMDRF/SaMD WG/N23 – Software as a Medical Device (SaMD): Application of Quality Management System;
- Medical Device Single Audit Program (MDSAP).

A quality management system must meet the requirements of MDR Article 10 for all risk classes. For the risk Class IIa and higher, a QMS also needs to meet the requirements of ISO 13485. For the risk **Class I**, compliance with **ISO 13485 is voluntary**.

4.2 Person Responsible for Regulatory Compliance (PRRC)

- MDR – Article 15 – Person responsible for regulatory compliance;
- MDCG 2019-7 Guidance on Article 15 of the Medical Device Regulation (MDR);
- Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Quality Management System

The PRRC is responsible for compliance with MDR as described in Article 15, just like the Management Representative is responsible for the quality management system. Therefore, those two functions are often performed by a single person. MDCG 2019-7 Guidance on Article 15 of the Medical Device Regulation (MDR) gives more information on how to perform the PRRC function.

The PRRC has to be registered in EUDAMED, with their contact details visible to the general public. Therefore, it is advised to use a common email address and phone number. The PRRC can have personal liabilities, but this is arranged by the local legislation of each Member State. When there is more than one PRRC, the division of responsibilities must be described. Small and Medium Enterprises (SMEs) may outsource the PRRC function. An SME is a firm that has less than 50 employees and a turnover of less than €10 million.

Information Security Management System

5.1 Introduction

- DiGAV;
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

DiGAV obliges DiGA manufactures to ensure compliance of their IT security management systems with ISO/IEC 27001. Compliance is proved with an ISO/IEC 27001 certificate.

Such a system requires:

- Establishment of corporate goals;
- Evaluation of the systems by top management (management review);
- Internal audits;
- Control of documents and records;
- Resource management (employees, infrastructure);
- Process-oriented approach.

The requirements for IT security management overlap with the requirements for quality management systems (typically compliant with ISO 13485 but not mandatory for Class I).

Information Security Management System

These similarities are also reflected in standard operating procedures (SOPs):

QMS according to ISO 13485	ISMS according to ISO/IEC 27001
Quality management manual	(X)
Quality objectives	(X)
Organizational chart, definition of roles	X
SOP management review/SOP performance measurement	X
SOP data analysis/SOP performance measurement	X
SOP control of documents and records	X
SOP CAPA (incl. ISMS)	X
SOP internal and external audits	X
SOP incident reporting	(X)
SOP IT infrastructure	X
SOP computer system validation	X
SOP recruiting and training	X
SOP purchasing and supplier management	X
SOP software development	X
SOP support, feedback handling, complaint handling	(X)

Therefore, DiGA manufacturers should establish one integrated management system rather than two isolated systems.

6.1 Introduction

- MDR Annex II: Technical documentation;
- MDR Annex III: Technical documentation on post-market surveillance;
- Recommendation NB-MED/2.5.1/Rec5: Technical Documentation;
- GHTF-SG1-N011R17: Summary Technical Documentation for Demonstrating Conformity to the Essential Principles of Safety and Performance of Medical Devices (STED).

Technical documentation (MDR Annex II) gives the details of what needs to be documented for CE-marking certification of a medical device.

Along with that, technical documentation for the software development life cycle, cyber security, and interoperability needs to be added.

Technical documentation consists of the following elements:	

Device description and specification, including variants and accessories:	• Device description:
	  ◦ Name;
	  ◦ UDI;
	  ◦ Patient population and their medical condition;
	  ◦ Principle of operation;
	  ◦ Qualification of the medical device;
	  ◦ Classification of the medical device;
	  ◦ Explanation of innovations;
	  ◦ Description of accessories and, if applicable, system modules/components;
	  ◦ Configurations and variants;
	  ◦ Parts and components;
	  ◦ Raw materials and elements with human body contact;
	  ◦ Technical specifications.
	• Reference to previous and similar generations of the device.

Technical Documentation (Technical File)

Information to be supplied by the manufacturer:	• Device with a packaging label and instructions for use.
Design and manufacturing information:	• Description of the development process; • Description of the manufacturing processes; • Software validation of development tools; • Manufacturing validations, monitoring, and final device testing; • Information about all suppliers and subcontractors that perform development, manufacturing, hosting, installation, and maintenance activities.

General safety and performance requirements (Annex I):	• Identification of applicable GSPRs in MDR Annex I;
	• Evidence of conformity with GSPRs, including:
	  ◦ Methods used to demonstrate conformity;
	  ◦ Applicable standards, Common Specifications, and other requirements;
	  ◦ Links to documents demonstrating conformity.

Benefit-risk analysis and risk management:	• Benefit-risk analysis MDR Annex I (1, 8), where benefits outweigh risks and the risks are reduced as much as possible and acceptable; • Risk Management MDR Annex 1 (3), as required by ISO 14791.

Device verification and validation:	• Pre-clinical data:
	  ◦ System requirements test plan and report.
	• Clinical data:
	  ◦ Clinical evaluation plan and report;
	  ◦ PMCF plan and report.
	• Description of combination/configuration with connected devices.

Technical documentation on post-market surveillance (Annex III):	• Post-market surveillance plan; • Post-market surveillance report (Class I); • Periodic safety update report (Class IIa, Class IIb).

6.2 General Safety and Performance Requirements (GSPR)

6.2.1 Introduction

- MDR – Annex I – General safety and performance requirements;
- COCIR Recommendation Applicability of EHSR of the Machinery Directive (2006/42/EC) to Medical Devices;
- MedTech Europe: The use of state-of-the-art standards in the absence of harmonizedstandards under the IVD and Medical Devices Regulations (IVDR/MDR);
- MDCG 2021-8 – Annex 6 – Checklist of general safety and performance requirements, standards, common specifications and scientific advice.

GSPR in MDR Annex I stands for General Safety and Performance Requirements. These requirements must be met by MDSW if they are applicable. It is good practice to put GSPR requirements on a checklist.

6.3 Software Development Life Cycle

6.3.1 Introduction

- MDR – Annex I – 17.1 – Repeatability, reliability and performance;
- MDR – Annex I – 17.2 – State of the art, software development life cycle, riskmanagement, (cyber)security and verification and validation;
- MDR – Annex I – 17.3 – Mobile platforms;
- MDR – Annex I – 17.4 – Hardware, IT networks, (cyber)security;
- IEC 62304: Medical Device Software LifeCycle Processes;
- IEC 82304-1: Health software requirements for product safety;
- HL7 Consumer Mobile Health Application Functional Framework.

The following standards must be considered for the software development life cycle and usability:

- IEC 62304 – Software life cycle processes. This standard must be followed during the entire software development in addition to ISO 13485 for the QMS. Note: ISO 14971 requires reducing risks as much as possible, which is more restricting than IEC 62304 Amendment 1, so ISO 14971 must be applied here;

- IEC 82304-1: Health software – General requirements for product safety. This standard is for stand-alone health apps or clinical information systems and can be used in addition to IEC 62304 for MDSW, if applicable. The standard also describes requirements of a higher level, such as security aspects;

- IEC 62366-1 is a usability standard for software, and IEC 60601-1-6 is a usability standard for MDSW integrated into electronic equipment, which can be used in addition to IEC 62366-1, if applicable.

Software safety classification according to IEC 62304:2006/Amd 1:2015

A software system belongs to Class A if:

- it cannot contribute to a hazardous situation;

- it can contribute to a hazardous situation that does not result in unacceptable risk after consideration of risk control measures external to the software system.

A software system belongs to Class B if:

- it can contribute to a hazardous situation that results in unacceptable risk after consideration of risk control measures external to the software system, and the resulting possible harm is a non-serious injury.

A software system belongs to Class C if:

- it can contribute to a hazardous situation that results in unacceptable risk after consideration of risk control measures external to the software system, and the resulting possible harm is death or a serious injury.

Technical Documentation (Technical File)

For a software system initially classified as Software Safety Class B or C, the manufacturer may implement additional risk control measures external to the software system (including revising the system architecture containing the software system) and subsequently assign a new software safety classification to it.

HA belongs to Class A

The table below shows the documents that the company provides for this class of software safety.

Document	Class A	Class B	Class C
Software Description	X	X	X
Software Development Plan	X	X	X
Software Test Plan	X	X	X
Quality management manual	X	X	X
Software Risk Management Plan	X	X	X
Software Configuration Management Plan	X	X	X
Software Requirements Specifications (SRS)	X	X	X
Software Specification Review	X	X	X
Traceability Analysis	X	X	X
Verification and Validation Documentation	X	X	X
Revision Level History	X	X	X
Software Architecture (Architecture Design Chart)		X	X
Software Architecture Review		X	X
Software Detailed Design		X	X

Software Detailed Design Review			X
Software Unit Verification Test Protocol		X	X
Software Unit Verification Test Report		X	X
Software Integration Test Protocol		X	X
Software System Test Report		X	X
Software Release Report		X	X
Software Maintenance Plan	X	X	X
Software Risk Analysis Report	X	X	X
Software Development Environment Description		X	X
Unresolved Anomalies (Bugs or Defects)		X	X

6.3.2 Software Development Life Cycle Documentation

- Software Description;
- Software Development Plan;
- Software Test Plan;
- Software Risk Management Plan;
- Software Configuration Management Plan;
- Software Requirements Specifications (SRS);
- Software Specification Review;

Technical Documentation (Technical File)

- Traceability Analysis;
- Verification and Validation Documentation;
- Revision Level History;
- Software Maintenance Plan;
- Software Risk Analysis Report.

6.4 Risk Management

6.4.1 Introduction

- MDR – Annex 1 (1) – Acceptable risk;
- MDR – Annex 1 (2) – Risk reduction;
- MDR – Annex 1 (3) – Risk Management;
- MDR – Annex I (4) – Risk Controls;
- ISO 14971:2019 – Application of risk management to medical devices;
- IEC/TR 80002-1: Guidance for applying ISO 14971 to software;
- NPR 5326: Risk management during development and maintenance of custom software (Dutch).

ISO 14971:2019 describes a systematic approach to risk management for medical devices. IEC/TR 80002-1 gives guidance for applying ISO 14971 to software. ISO 14971 is used to obtain a safe medical device so that:

- there are no unacceptable risks.
- there is a positive benefit-risk ratio, which is analyzed in the clinical evaluation.

6.4.2 Risk Management Plan

ISO 14971:2019 requires a risk management process for the entire product life cycle. This includes planning and execution of all relevant tasks, activities, procedures, and responsibilities, both during product development and when the product is already on the market. This also includes design changes, new risks, changes in the benefit-risk ratio, etc. In order to obtain such information, a post-market surveillance system is needed.

6.4.3 Risk Management Report

Prior to release for commercial distribution of a medical device, the manufacturer must carry out a review of the risk management process. This review must at least ensure that:

- the risk management plan has been appropriately implemented;
- the overall residual risk is acceptable;
- appropriate methods are in place to obtain relevant production and post-production information.

6.4.4 Risk Management Documentation

- Risk Management Plan;
- Risk Management Report.

6.5 Clinical Evidence

6.5.1 Introduction

Clinical evaluation:

- MDR – Article 6 – Clinical evaluation;
- MDR – Annex XIV – Part A – Clinical evaluation;
- MDCG 2020-13 Clinical evaluation assessment report template;
- MDCG 2020-6 Guidance on sufficient clinical evidence for legacy devices;
- MDCG 2020-5 Guidance on clinical evaluation – Equivalence;
- MDCG 2019-9 Summary of safety and clinical performance;
- MEDDEV 2.7/Rev. 4: Clinical evaluation according to the MDD; this document still containsvaluable information.

MDSW clinical evaluation:

- MDCG 2020-1 Guidance on clinical evaluation (MDR);
- IMDRF/SaMD WG/N41 Software as a Medical Device (SaMD): Clinical Evaluation;
- IMDRF/SaMD WG (PD1)/N41R3 Software as a Medical Device (SaMD): Clinical Evaluation (proposed document).

Technical Documentation (Technical File)

MDSW clinical evaluation:

- MDR – Article 61 (4-6) – Clinical investigations;
- MDR – Articles 62-82 – Clinical investigations;
- MDR – Annex XV – Clinical investigations;
- MDCG 2020-10 Guidance on safety reporting in clinical investigations;
- MDCG 2021-6 Questions & Answers regarding clinical investigation;
- ISO 14155: Clinical investigation of medical devices for human subjects – Good clinical practice.

HA must have sufficient clinical evidence that is therefore seen as the most important element to get market access. The clinical evaluation is a scientific approach to create this evidence and has a long list of detailed requirements in MDR and the applicable guidance. MDCG guidance for clinical evaluation assessment reports is used to ensure the clinical evaluation meets these requirements.

In order to bring HA to the market, there must be evidence that the device is safe and performs the functions it is designed to perform. Such evidence consists of two parts:

Technical Evidence coming from testing, for instance, and clinical evidence coming from the Clinical Evaluation Report.

Technical Documentation (Technical File)

The clinical evaluation is a systematic and scientific analysis process. Its flow is described in MDR Annex XIV Part A and in MEDDEV 2.7/Rev. 4. In order to conduct clinical evaluation, clinical data for the device or for its analogs – also called equivalent devices – is collected. Clinical data can be obtained from clinical investigations, post-market clinical follow-up studies, or post-market surveillance studies. The clinical data is analyzed, and the conclusions are called clinical evidence. When possible, clinical evidence may be replaced by technical evidence for Class IIb devices or lower (see MDR Article 61(10)).

The clinical evaluation aims to examine and evaluate clinical data to verify the clinical safety and performance of the medical device. The results of the clinical evaluation are used to assess whether the risks associated with the use of the medical device are acceptable in relation to the expected benefit. The manufacturer must keep the clinical evaluation up to date throughout the entire life cycle of the product by repeating the literature study and conducting post-market surveillance. The manufacturer must update the PMCF assessment report for Class III and implantable medical devices annually. For lower class devices, there must be at least a plan for PMCF studies – Article 61 (11) and Annex XIV PartB.

During the clinical evaluation, it is assessed whether there is sufficient clinical evidence for the safety and performance of the device. At least a literature study on the medical device in clinical practice must be performed. If clinical evidence is still insufficient, then a clinical investigation needs to be carried out. Clinical evidence is included in technical documentation.

The results of the clinical investigation must be reported in EUDAMED. For implantables and Class III devices, it is also reported in a Summary of Safety and Clinical Performance, and for devices of Class IIa and higher, it is also reported in a Periodic Safety Update Report.

6.5.2 Clinical Evidence Documentation

- Clinical Evaluation Plan (CEP, Annex XIV, Part A, 1.) describing the procedure for clinical evaluation to demonstrate the benefit-risk ratio based on the state of the art in medicine;
- Clinical Evaluation Report (CER, Article 61 (12));
- Clinical Development Plan (CDP, Annex XIV, Part A, 1a & 1d);
- Clinical Investigation Plan (CIP, Annex XV, 3);
- Post-Market Clinical Follow-Up (PMCF) Plan (Annex XIV, Part B) or a justification as to why a PMCF is not applicable (outlined in the Post-Market Surveillance (PMS) Plan);
- Periodic Safety Update Report (PSUR) for Class IIa (biannual update) and Class IIb (annual update) (Article 86);
- Clinical Evaluation Assessment Report (CEAR, Annex VII, Section 4.6, to be compiled by the notified body).

For MDSW Class I, clinical evaluation can be covered by performance testing.

6.6 Usability

6.6.1 Introduction

- MDR – Article 83 (3f) – Identification of PMS data to improve usability;
- MDR – Annex I (5) – Reduce risks related to use error;
- MDR – Annex I (14.2) – Reduce risks caused by design;
- MDR – Annex I (14.6) – Ergonomic principles;
- MDR – Annex I (23) (23) – Information supplied with the product;
- IEC 62366-1a: Application of usability engineering to medical devices;
- IEC 62366-2 – Section 15.3: Design software user interfaces.

IEC 62366-1 is a usability standard for software. It must be considered together with ISO 14971: Risk management. IEC 62366-1 describes the usability engineering process aimed at ensuring an acceptable risk for MDSW. IEC/TR 62366-2 explains in more detail how usability engineering can be designed and can be used next to IEC 62366-1.

The usability engineering process includes the following elements:

- Usability engineering planning

Technical Documentation (Technical File)

The Usability Engineering Plan describes the project and provisions for implementing the usability engineering process.

- Usability input data

The project starts with collecting the design input data for usability, such as:

- MDR and other regulatory requirements, like those for instructions for use or labeling;
- user requirements from product managers, application specialists, sales managers, etc.;
- data from previous projects;
- feedback from users on previous versions of medical devices;
- analysis of similar medical devices.

- Use specification

The use specification contains information about:

- intended purpose;
- indications and patient groups;
- user profiles;
- use environment;
- operating principles.

- Identification of characteristics for safety

Technical Documentation (Technical File)

The usability analysis is performed in parallel with the ISO 14971 risk management process. This step defines:

- primary operating functions of the device;
- use scenarios;
- possible use errors.

- Identification of hazardous situations

This step defines:

- the use specification;
- data from comparable devices or previous generations of the device;
- user errors defined in the previous step.

- Identification of hazard-related use scenarios

This step defines the sequence of events and the related hazards.

- Selection of hazard-related scenarios for summative evaluation

This step defines hazard-related scenarios for the summative evaluation based on objective criteria. Usually, these are the scenarios that have the most impact on the benefit-risk ratio.

- Identification of mitigations and the User Interface Specification

The risks related to the use scenarios are evaluated for severity, frequency, and possibly detectability. During this step, mitigation actions are defined. The mitigation actions are documented in the User Interface Specification:

- Changes in user-interface design, including warnings like notification screens;
- Training of users;
- Information on the instructions for use and labeling.

- Formative evaluation

The formative evaluation is performed during the design phase. Initially, internal employees can evaluate the product, but in later stages the users take over this responsibility. The methods of evaluation depend on the context: questionnaires, interviews, presentations of mock-ups, or observation of the use of prototypes.

- Summative evaluation

The summative evaluation is performed at the end of the design phase. It can be done after the verification or during the validation of MDSW. The summative evaluation needs to be done with the input of users. FDA guidance provides sample sizes for each user group. The evaluation needs to be done in a (simulated) use environment.

6.6.2 Usability Documentation

- Usability Engineering File;
- Usability Engineering Plan;
- Use Specification;
- User Interface Evaluation Plan;
- User Interface Specification;
- Formative Evaluation;
- Summative Evaluation.

6.7 Cyber Security

6.7.1 Introduction

General:

- MDR – Annex I (14.2.(d)) – MDSW and IT networks interaction risks;
- MDR – Annex I (17.2) – Software development life cycle in accordance with the state of the art, risk management, (cyber)security and verification and validation;
- MDR – Annex I (17.3) – Mobile platforms;
- MDR – Annex I (17.4) – Hardware, IT networks, (cyber)security;
- MDR – Annex I (18.8) – Unauthorized access;
- MDCG 2019-16 Medical Devices: Cybersecurity;
- IMDRF/CYBER WG/N60 Principles and Practices for Medical Device Cybersecurity;
- ENISA NIS directive All devices: Network and Information Security;
- GDPR (General Data Protection Regulation);
- DiGAV.

Technical Documentation (Technical File)

Requirements:

- ISO 27001 – Information technology – Security techniques – Information security management systems – Requirements;
- IEC 81001-5-1:2021 Health software and health IT system safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle;
- BSI-Standard 200-1: Information Security Management Systems (ISMS);
- BSI-Standard 200-2: IT Basic Protection Methodology;
- BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz;
- IEC 80001: Healthcare IT networks: risk management, IT networks;
- IEC 80001-1: Healthcare IT networks;
- IEC/TR 80001-2-2-2: Healthcare IT networks;
- ISO 27799: Healthcare IT networks: information security, management;
- BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths;
- BSI TR-02102-2: Cryptographic Mechanisms: Use of Transport Layer Security (TLS);
- TR-03107-1. Electronic Identities and Trust. Services in E-Government.

An indicative list of security capabilities for MDSW:

- Automatic logoff;
- Audit controls;
- Authorization;
- Configuration of security features, cyber security, product upgrades, personal data de-identification, data backup, and disaster recovery emergency access;
- Personal data integrity and authenticity and malware detection/protection;
- Node authentication;
- Person authentication;
- System and OS hardening;
- Security and privacy guides;
- Personal data storage, confidentiality transmission, and confidentiality transmission integrity.

6.7.2 GDPR

HA will handle patient data, so GDPR (General Data Protection Regulation) must be met.

6.8 IFUS, Labels, Brochures, and Website

6.8.1 Introduction

- MDR – Annex I (23) – Label and instructions for use;
- MDR – Annex I (23.4 f) – MDSW and accessory selection;
- MDR – Annex I (23.4 ab) – MDSW minimum requirements;
- MDEG 2008-12- II-6.3 Mandatory Languages Requirements for Medical Devices;
- ISO 15223-1 Medical Devices – Symbols to be used with medical device labels, labeling and information to be supplied – Part 1: General requirements;
- EN 1041 – Information supplied by the medical device manufacturer;
- ISO 20417: Information to be supplied by the manufacturer;
- ISO's Online Browsing Platform (OBP) – Symbols;
- IEC 82304-1: Health software requirements for product safety;
- MedTech Europe – Use of Symbols to Indicate Compliance with the MDR.

The requirements for labels, packaging, and instructions for use (IFU) are described in MDR Annex I Section 23. There are many additional requirements for labels and IFU, such as Implant Cards, but most of them are not applicable to MDSW. IEC 82304-1 contains additional requirements for IFU:

- Start-up and shut-down instructions (§ 7.2.2.5 and 7.2.2.6);
- Disposal instructions for the software in relation to Information Security and Privacy (§ 7.2.2.9);
- IT network specifications and risks (§ 7.2.3.2).

The symbols that can or must be used are described in ISO 15223-1.

6.8.2 Health Software Documentation

- Manufacturer contact information;
- Product identification and version;
- Operating instructions with the description of HA;
- Security alerts;
- Installation guide;
- Switch-on and switch-off procedures;

Technical Documentation (Technical File)

- Operating instructions;
- Validation plan;
- Validation report;
- Notifications;
- Post-market communication on the health software product;
- Decommissioning and disposal of the health software product;
- Technical description, e.g., for network integration;
- Software problem resolution process.

6.9 UDI (Traceability) and EUDAMED

- MDR – Article 27 – Unique device identification system;
- MDR – Article 28 – UDI database;
- MDR – Annex VI – UDI database;
- MDCG 2018-1 Guidance on Basic UDI-DI and changes to UDI-DI;
- MDCG 2018-3 Guidance on UDI for systems and procedure packs;
- MDCG 2018-4 Definitions/descriptions and formats of the UDI core elements for systems or procedure packs;
- MDCG 2019-1 MDCG guiding principles for issuing entities rules on Basic UDI-DI;
- EU UDI System – FAQs;
- MedTech Europe's Guidance on Basic UDI-DI Assignment;
- HL7 ANSI/HL7 UDI, HL7 Cross Paradigm Implementation Guide: UDI Pattern.

The unique device identification (UDI) code is used to identify a medical device. This is extremely important when a recall or warning of the product has to take place. Keeping track of medical device production and use is called traceability. The UDI also has many secondary uses, like managing the logistics chain or stock.

The UDI code will be publicly available after the registration in the EUDAMED database.

Technical Documentation (Technical File)

For UDI used for MDSW, there are specific requirements in Annex VI Part C and MDCG 2018-5:

- The UDI (UDI-DI + UDI-PI) is usually given at the system level of the software if the intended use and risk class is the same;
- The software identification on the label is part of the UDI-PI;
- After certain software changes, a new UDI-DI must be assigned;
- The human-readable form can be stored in software menus. If there is no userinterface, other ways have to be used, e.g., an application programming interface (API).

A new UDI-DI is required when there are:

- any changes of the basic UDI-DI;
- any changes that impact the original performance, safety, or the interpretation of data;
- any changes to the name or trade name, version or model number, critical warnings, or contraindications.

Minor software revisions – e.g., bug fixes not related to safety or security – require not a new UDI-DI but a new UDI-PI.

By 26 May 2023: UDI: Class IIa/IIb products must be UDI-marked – Article 123 (3f).

By 26 May 2025: UDI: Class I products must be UDI-marked – Article 123 (3f).

6.10 Post-Market Obligations

6.10.1 Introduction

Post-Market Surveillance (PMS):

- MDR – Article 83 – Post-market surveillance system of the manufacturer;
- MDR – Article 84 – Post-market surveillance plan;
- MDR – Article 85 – Post-market surveillance report;
- MDR – Article 86 – Periodic safety update report (PSUR);
- MDR – Article 92 – Electronic system on vigilance and on post-market surveillance;
- MDR – Annex III – Technical documentation on post-market surveillance;
- ISO/TR 20416 – Post-market surveillance for manufacturers;
- Setting up PMS (original title: Vormgeven PMS voor medische hulpmiddelen onder de MDR en de IVDR).

Post-Market Clinical Follow-up (PMCF) and Registries:

- MDR – Article 61(11) – Post-market clinical follow-up;
- MDR – Annex XIV – Part B – Post-market clinical follow-up;

- MDCG 2020-7 Post-market clinical follow-up (PMCF) Plan Template;
- MDCG 2020-8 Post-market clinical follow-up (PMCF) Evaluation Report Template;
- IMDRF/Registry WG/N46. Tools for Assessing the Usability of Registries in Support of Regulatory Decision-Making;
- IMDRF/Registry WG/N42FINAL:2017. Methodological Principles in the Use of International Medical Device Registry Data.

6.10.2 Post-Market Surveillance and Clinical Follow-Up Documentation

- Post-Market Surveillance Plan;
- Post-Market Surveillance Report (for Class I);
- Periodic Safety Update Report (PSUR) (for Class IIa and IIb);
- Post-Market Clinical Follow-Up Plan;
- Post-Market Clinical Follow-Up Report.

6.11 Complaint Handling, Vigilance Reporting, and Market Surveillance

6.11.1 Introduction

Feedback and complaint handling:

- ISO 13485 – 8.2.1 Feedback;
- ISO 13485 – 8.2.2 Complaint handling.

Feedback and complaint handling:

- MDR – Article 80 – Recording and reporting of adverse events that occur during clinical investigations;
- MDR – Article 87 – Reporting of serious incidents and field safety corrective actions;
- MDR – Article 88 – Trend reporting;
- MDR – Article 89 – Analysis of serious incidents and field safety corrective actions;
- MDR – Annex III – Technical documentation on post-market surveillance;
- MEDDEV 2.12-1 Rev. 8 Guidelines on a Medical Devices Vigilance System and Additional Guidance Regarding the Vigilance System;
- GHTF SG2 document N54 Appendix C: Global Guidance for Adverse Event Reporting for Medical Devices.

Market surveillance:

- MDR – Articles 90-100 – Market surveillance;
- EU regulation 2019/1020 on market surveillance and compliance of products.

The complaint handling and vigilance reporting processes can be established in multiple ways. Below are the typical elements of these processes:

- Feedback;
- Complaint handling;
- Vigilance reporting;
- Trend Report;
- Periodic Safety Update Report (PSUR) (MDR Article 86);
- Market surveillance.

7.1 Safety and Suitability for Use

- DiGAV;

- The Fast-Track Process for DiGA according to Section 139e SGB V. A Guide for Manufacturers, Service Providers and Users.

The SGB V requires manufacturers of DiGA to prove the safety of the device and its suitability for use as part of the application procedure. Compliance with requirements concerning the safety of the device and suitability for use is regarded as proven with a valid EG-Certificate of conformity which is the declaration of conformity of the manufacturer. As a rule, the BfArM only carries out checks on the formal legality of the CE marking for this requirement.

CE marking for MDSW Class I is required to meet this requirement.

7.2 Requirements for Data Protection and Data Security

1. DiGA must comply with the legal requirements for data protection and the requirements for data security according to the state of the art, taking into account the type of data processed and the associated protection levels and requirements.

2. In the context of DiGA, personal data may only be processed on the basis of the consent of the insured person pursuant to Article 9 Paragraph 2 letter a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) (General Data Protection Regulation) (OJ L 119 of 04.05.2016, p. 1) exclusively for the following purposes:

a) The intended use of DiGA;

b) The proof of positive supply effects in the context of a test according to Section 139e Paragraph 4 of Book V of the Social Code;

c) The proof of agreements according to Section 134 Paragraph 1 Sentence 3 of Book V of the Social Code;

d) Permanent guarantee of the technical functionality, user-friendliness, and further development of DiGA (consent to data processing pursuant to Sentence 1 Number 4 must be obtained separately from consent to data processing for purposes pursuant to Sentence 1 Number 1 to 3. Data processing authorizations according to other regulations remain unaffected.).

3. The processing of personal data for the purposes according to Paragraph 2 may only take place in Germany, a member state of the European Union (according to Article 35 Paragraph 7 of Book I of the Social Security Code), or, if there is an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679, in any other country.

4. Processing of personal data for purposes other than those specified in Paragraph 2 Sentence 1, in particular for advertising purposes, is excluded. The authority to process data in accordance with other regulations under Paragraph 2 Sentence 3 remains unaffected.

5. The manufacturer of DiGA obliges all persons working for them and having access to the personal data of the insured persons to maintain confidentiality.

6. The details of the requirements according to the above paragraphs are determined pursuant to Annex 1. The manufacturer must include the declaration with their application according to Annex 1. If the specifications in Annex 1 prove to be unsuitable with regard to the properties of DiGA, DiGA may deviate from the specifications in Annex 1 in individual cases. If the legal specifications for data protection and the requirements for data security are state-of-the-art, a different implementation can be applied in the same way. In their application, the manufacturer is expected to explain the deviation from the specifications in Annex 1 and justify it.

7. From 1 January, 2025, DiGA must meet the data security requirements specified by the Federal Office for Information Security in accordance with Section 139e Paragraph 10 of Book V of the Social Code, instead of the data security requirements under Paragraph 6.

8. From 1 August, 2024, DiGA must shift from the data protection requirements according to Paragraph 6 to meet the test criteria specified by the Federal Institute for Drugs and Medical Devices according to Section 139e Paragraph 11 of Book V of the Social Code for the requirements to be verified to implement data protection.

As of 2023, manufacturers are not only required to have a certified IT security management system but also a data security and data protection certification.

7.3 Requirements for Quality

1. DiGA must be designed in such a way that they follow the requirements for technical and semantic interoperability. In particular, DiGA must enable processed data to be exported in suitable interoperable formats and used in the context of care. In addition, DiGA must use interoperable interfaces if, as part of the intended use, it exchanges data with medical devices used by the insured person or with sensors worn by the insured person for measuring and transmitting vital signs (wearables).

Requirements for DiGA

2. DiGA must be designed in such a way that they are robust against disruptions and operating errors.

3. DiGA must be designed in such a way that the consumer protection requirements are met in accordance with Annex 2. In particular, DiGA must provide the insured person with information on its scope of functions, purpose, and contractual conditions of use before they start using it.

4. DiGA must be free of advertising.

5. DiGA must be designed in such a way that the insured person can use them easily and intuitively. DiGA must provide for measures to support the insured person for the duration of DiGA in the directory, at least for the period of use of DiGA at the expense of the statutory health insurance companies according to Section 33a Paragraph 1 of Book V of the Social Code.

6. DiGA must follow the accessibility requirements in accordance with Annex 2.

7. If the purpose of using DiGA requires that service providers are involved in the use of the application, the application must ensure that the service providers are informed and supported in an appropriate manner.

8. The medical content used by DiGA must correspond to the generally recognized state of medical knowledge. If DiGA provides the insured person with health information, the health information must also correspond to the generally recognized professional standard and be prepared in a way that is appropriate for the target group.

9. DiGA must include measures to support patient safety.

10. The details of the requirements according to the above paragraphs are determined according to Annex 2. If the specifications of Annex 2 prove to be unsuitable with regard to the properties of DiGA, DiGA can deviate from the specifications of the annex in individual cases if the requirement is equally met by a different implementation. In their application, the manufacturer is expected to explain the deviation from the specifications in Appendix 2 and justify it.

11. The manufacturer shall include the declaration with their application in accordance with Appendix 2.

7.3.1 Specifications for Interoperability

Interoperable formats according to Requirement 1 are definitions for the semantic and syntactic interoperability of data in the electronic patient record according to Section 355 Paragraph 2a of Book V of the Social Code. As long as no determination is made for the semantic and syntactic interoperability of data in the electronic patient file according to Section 355 Paragraph 2a of Book V of the Social Code, open, internationally recognized interface and semantic standards and profiles are provided by the manufacturer of DiGA via open, international recognized interface and semantic standards as interoperable formats. According to Sentence 2, the manufacturer must publish the profiles they have provided for free use in a recognized directory.

7.3.2 Interoperability of DiGA with Electronic Patient Record

1. From 1 January 2024, DiGA must be designed in such a way that the data processed by DiGA can be transmitted to the insured person's electronic patient file with the consent of the insured person in accordance with Section 341 of Book V of the Social Code. From 1 January 2023, DiGA must have the interface specified by the Gesellschaft für Telematik for data exchange in accordance with Section 354 Paragraph 2 Number 6 of Book V of the Social Code.

2. From 1 January 2024, DiGA will enable data to be exported to the electronic patient file in accordance with a specification for the semantic and syntactic interoperability of data in the electronic patient file in accordance with Section 355 (2a) of Book V of the Social Code.

The manufacturers of digital health applications shall implement the updates to the specifications pursuant to Section 355 (2a) of the Fifth Book of the Social Code within six months of their publication.

7.4 Interoperability

- MDR – Article 2 – Definition (26) – Interoperability;
- MDR – Annex I (14.5) – Interoperability;
- DiGAV – Section 6 – 6a.

Requirements for DiGA

In order to be listed in the directory, the manufacturer of DiGA needs to prove that it is interoperable regarding three selected issues:

- DiGA allows the insured person to export therapy-relevant extracts of the data collected via DiGA in human-readable and printable form so that they can use them for their purposes or pass them on to a physician;

- DiGA allows the insured person to export the data collected from DiGA in a machine-readable, interoperable format so that the insured person or a third party authorized by the insured person can further process this data via other digital products. In the future, it must also be possible to connect this interface to the ePA;

- If DiGA obtains data from medical devices used by the insured person or sensors worn by the insured person for the measurement and transmission of vital signs (wearables), it also communicates with these devices via an interoperable interface.

In the figure below, green arrows point to the interoperability interfaces to be implemented. The dotted arrows point to future enhancements already set, which, however, must only be implemented after the ePA has been established in the healthcare system. Gray arrows point to optional interfaces, i.e. DiGA can include them, but they are not subject to any specifications or restrictions by DiGAV. The manufacturer can also provide redundant, additional implementations for all interfaces shown with green arrows in the figure. It is only important that at least one option is implemented here for exporting data or interacting with connected devices, which corresponds to the interoperability specifications formulated in Annex 2 of DiGAV.

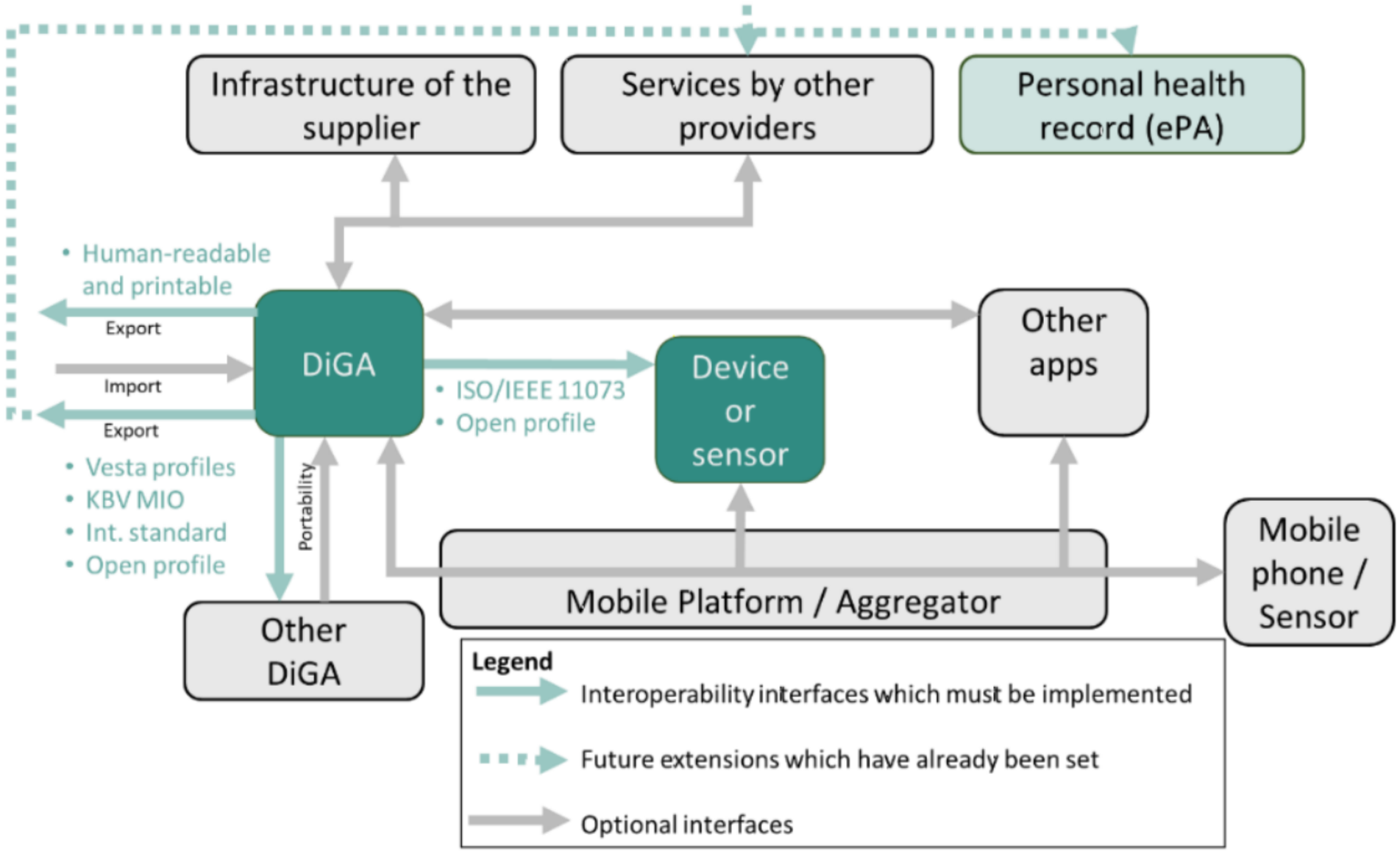

Figure 2 – IOP for DiGA. Source: BfArM.

7.5 Evidence of Positive Healthcare Effects

DiGAV requires evidence of positive healthcare effects. The regulation defines them as "Either [a] medical benefit or patient-relevant structural and procedural improvements in care."

The following steps are performed for clinical evaluation:

- Determine claims

Requirements for DiGA

In order to be able to prove positive healthcare effects, manufacturers need to specify the performance and acceptance criteria ("claims") as quantitatively as possible. This sounds obvious, but this is where manufacturers often make mistakes. For example, claims may be:

- not specific (or quantitative) enough to design a study,
- formulated too broadly and/or too demanding, which is why the proof can be provided neither on time nor within the scope of the given means,
- formulated too narrowly and/or not demanding enough, so the benefit is too small for DiGA to be included in the directory.

- Decide on the timing

Once these claims are specified, manufacturers need to decide on whether to seek direct listing or just provisional listing in the directory. The latter gives the manufacturer an additional year to complete their clinical study but does not guarantee final acceptance.

An advantage of this additional year is that GKV funds already reimburse DiGA, and the manufacturer is allowed to set the price. Negotiations with GKV funds are conducted after the trial year. In this way, the expensive study can be at least partially financed.

- Plan the study

Then, the study needs to be planned, and the evaluation concept of the study design has to be defined.

Manufacturers must contact BfArM at the end of this step or even earlier.

A prerequisite for the main study of DiGA is a pilot study with systematic data evaluation.

- Provide proof of benefit

Proof of the positive healthcare effects is provided – as described in the study plan (see above) – by collecting the clinical data within the framework of corresponding comparative studies, as required by DiGAV in Section 10 (only available in German).

If the manufacturer wants to go into trials first, they start with a systematic data evaluation or pilot study. This should correspond to the main study in all essential details. Only the number of cases may be somewhat smaller. The manufacturer then submits the outputs of the pilot study together with the evaluation concept when applying.

The manufacturer must register their study in BfArM.

7.6 Listing in DiGA Directory

7.6.1 Initial Interview

Andersen recommends DiGA manufacturers benefit from BfArM's offer of consultation without waiting until the application is submitted before contacting the authority. A good time for an initial consultation is when the intended use, MDSW class, and clinical evaluation strategy are defined.

- Preparation

In order to ensure the best possible coordination with the authority, manufacturers need to thoroughly prepare for the interview, as well as thoroughly prepare their documents:

Requirements for DiGA

- Product presentations, including the intended use specification;
- Justification for qualification and classification;
- The list of claimed positive healthcare effects;
- The project plan (product development, certification, study, and marketing);
- The study plan, at least for the pilot study;
- The list of questions for BfArM.

Manufacturers need to assemble their own expert group (product, regulatory, study design/statistics, medical) to sit opposite BfArM's expert group.

- Conversation management

In order to ensure that the interview is as efficient and effective as possible, manufacturers need to at least:

- coordinate their questions and agenda with BfArM in advance;
- introduce DiGA in the interview and solicit feedback on whether it seems interesting;
- solicit feedback on the study plan (pilot and/or main study) during the interview.

7.6.2 Application Submission

When all the above steps are successfully completed, the DiGA manufacturer may submit the application. For this purpose, BfArM has provided a completion guide (only available in German).

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

In the questionnaire listed below, the manufacturer is supposed to declare DiGA's compliance with the data protection and security requirements. The manufacturer confirms that the requirements have been met by marking it in the Applicable column. Data protection regulations and data security requirements are the basic requirements that must be met by all DiGA. The requirements for data security are additional requirements for DiGA with a very strict protection requirement that must be met by DiGA and which was determined as part of the required protection requirement analysis.

No.	Topic	Requirement	Applicable / Not applicable	Acceptable justification for "Not applicable"
Data protection				
1	GDPR as an applicable law	The processing of personal data by DiGA and its manufacturer is subject to Regulation (EU) 2016/679 and other data protection regulations.		
2	Consent	Is voluntary, specific, and informed consent to process personal data for the purposes specified in Section 4 (2) obtained from the data subject?		Consent is not required because the purpose of the processing results from a legal obligation of the DiGA manufacturer.
3	Consent	Is the consent and declaration given by the data subject express (given by the data subject actively and clearly)?		Consent is not required because the purpose of the processing results from a legal obligation of the DiGA manufacturer.
4	Consent	Can the data subject revoke given consent easily, barrier-free, at any time, and in an easily understandable way with effect for the future?		Consent is not required because the purpose of the processing results from a legal obligation of the DiGA manufacturer.
5	Consent	Is the data subject informed of the rights and possibilities to revoke the consent before giving it?		Consent is not required because the purpose of the processing results from a legal obligation of the DiGA manufacturer.

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

6	Consent	Before giving consent, was the data subject informed in a clear, understandable, user-friendly form appropriate to the target group about what categories of data are processed by DiGA or the manufacturer of DiGA and for what purposes?	Consent is not required because the purpose of the processing results from a legal obligation of the DiGA manufacturer.
7	Consent	Can the data subject retrieve the texts of the consents and declarations given at any time from DiGA or a source referenced in DiGA?	Consent is not required because the purpose of the processing results from a legal obligation of the DiGA manufacturer.
8	Earmarking	Are personal data processed by DiGA exclusively for the purposes mentioned in Section 4 Paragraph 2 Clause 1 or stated by other statutory data processing authorizations in accordance with Section 4 Paragraph 2 Clause 3?	
9	Data minimization and adequacy	Are the personal data processed via DiGA adequate for the purpose and limited to what is necessary for the purposes of the processing?	
10	Data minimization and adequacy	Has the manufacturer of DiGA ensured that the purposes of processing personal data by DiGA cannot reasonably be achieved by other, more data-efficient means to the same extent?	
11	Data minimization and adequacy	Are health-related data stored separately from data that is only required for billing?	
12	Data minimization and adequacy	Has the manufacturer of DiGA ensured that employees entrusted with non-product-related tasks do not have access to health-related data?	

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

13	Data minimization and adequacy	If the use of DiGA is not limited to a private IT system of the user, then: –were corresponding application scenarios explicitly taken into account in the data protection impact assessment? –is the insured person expressly informed that the use of DiGA in a potentially unsafe environment is associated with security risks that cannot be fully addressed by the manufacturer of DiGA? –when using DiGA on an IT system that is not only used by the insured person, is the storage of health-related data on this IT system – even temporary – completely prevented?	The use of DiGA is limited to a private IT system of the user.
14	Integrity and confidentiality	Does DiGA provide appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, deletion, falsification, disclosure, or unauthorized forms of processing?	
15	Integrity and confidentiality	Is the exchange of data controlled by DiGA between the end device of the person concerned and external systems encrypted according to the state of the art?	No personal data is exchanged between the end device of the person concerned and external systems.
16	Accuracy	Does DiGA provide technical and organizational measures to ensure that the personal data processed via DiGA are accurate and up-to-date?	
17	Accuracy	Does the manufacturer of DiGA take all reasonable measures to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are erased or rectified without delay?	
18	Necessity	Are personal data collected via DiGA only stored for as long as it is necessary to provide the promised functionalities or for other purposes directly resulting from legal obligations?	

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

19	Necessity	Are personal data no longer stored after the purposes specified in Section 4 Paragraph 2 Sentence 1 Numbers 1-4 are fulfilled?	The purpose of storage and the maximum storage period must be justified separately by the manufacturer, stating the reasons why these purposes represent legitimacy for the further storage of personal data.
20	Data portability	Does the manufacturer of DiGA provide mechanisms through which the data subject can exercise the right to data portability from DiGA and retrieve the personal data provided by the data subject to DiGA in a suitable format or in another that DiGA can transfer?	
21	Information requirements	Is the data protection declaration of DiGA easy to find, barrier-free, and available on the application website?	
22	Information requirements	Does the data protection declaration of DiGA contain all relevant information on the manufacturer and its data protection officer, the purpose of DiGA, the data categories processed for this purpose, how the manufacturer handles this data, the right to revoke given consent, and the possibilities for exercising the rights of data subjects? Does the manufacturer of DiGA adequately implement additional information obligations under Articles 13 and 14 of Regulation (EU) 2016/679?	
23	Information requirements	Can the data protection declaration of DiGA be easily found from DiGA or in DiGA even after it is installed?	
24	Information requirements	Can the data subject obtain information from the manufacturer of DiGA about the personal data stored to the extent specified in Article 15 of Regulation (EU) 2016/679?	

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

25	Information requirements	Does the data protection declaration of DiGA contain a comprehensible deletion concept that regulates the procedure for revoking consent and uninstalling DiGA, as well as the information about how to deal with claims for the deletion of data, the restriction of their processing, and compliance with the requirements specified in Articles 17-19 of the Regulation (EU) 2016/679?
26	Information requirements	Can the data subject request the manufacturer of DiGA to correct inaccurate or missing personal data concerning them and complete the data, if necessary?
27	Information requirements	Is the data subject informed of the data that may be lost as a result and of the right to data portability in accordance with Article 20 of Regulation (EU) 2016/679 before they delete their user account?
28	Privacy management	Has the manufacturer of DiGA implemented a procedure for regularly checking, assessing, and evaluating the effectiveness of the technical and organizational measures to ensure the security of processing, which covers all systems and processes used in connection with DiGA?
29	Privacy management	Has the manufacturer of DiGA committed all persons who have access to personal data for their work to secrecy?
30	Data protection impact assessment and risk management	Has the manufacturer of DiGA carried out a data protection impact assessment for DiGA? Has the risk analysis carried out in this way been transferred to the documented risk management processes after continuous reassessment of threats and risks?

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

31	Data protection impact assessment and risk management	Does the manufacturer of DiGA guarantee that the supervisory authority will be notified about a personal data breach within 72 hours of becoming aware of it?	
32	Data protection impact assessment and risk management	Has the manufacturer of DiGA implemented the requirements specified in Article 34 of Regulation (EU) 2016/679 to inform those affected in the event of data protection incidents?	
33	Obligation to provide evidence	Has the manufacturer of DiGA documented the data protection guidelines applicable to the company and trained its employees in their implementation?	
34	Obligation to provide evidence	Does the manufacturer of DiGA implement measures to ensure that it can be subsequently checked and determined whether and by whom personal data stored by the manufacturer of DiGA has been entered, changed, or removed?	
35	Obligation to provide evidence	Can the manufacturer of DiGA prove at any time that the data subject has given their consent to the processing of their personal data, provided the data processing is not based on another legal basis?	
36	Processing on behalf	Are personal data not passed on to processors at all via the DiGA or the manufacturer of DiGA, or only to processors who have sufficient trustworthiness and liability, implement appropriate mechanisms to protect the data they have taken over and are in a binding contractual relationship with the manufacturer of DiGA, which excludes a weakening of the commitments made to the insured person?	

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

37	Data transfer to third parties	Are no personal data passed on to third parties via DiGA or the manufacturer of DiGA, unless this is directly necessary for the fulfillment of purposes pursuant to Section 4 Paragraph 2 Sentence 1 Number 1 or the fulfillment of statutory provisions and is limited to these purposes?	
38	Processing abroad	Does the processing of health data, as well as personally identifiable inventory and traffic data, take place exclusively in Germany, another member state of the European Union, a state that is equivalent to this according to Section 35 Paragraph 7 of Book I of the Social Code, or on the basis of an adequacy decision according to Article 45 of the Regulation (EU) 2016/679?	
39	Other warranty goals	Is the concatenation of personal data across two or more DiGA technically impossible, or does the data subject have to give explicit, separately obtained, informed consent for a concatenation of data across two or more DiGA?	DiGA does not offer any technical possibility of linking or exchanging data with other DiGA.
40	Other warranty goals	Is it ensured that information from or about the data subject is not disclosed to the public or a group of people who cannot be defined by the data subject, or only as a result of an explicit, active action by the data subject who provides information tailored to the target group about the type of information disclosed and the possible circle of recipients?	DiGA does not support the disclosure of information from or about the data subject to the public or a group of people who cannot be restricted by the data subject.

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

Data security			
Basic requirements that apply to all DiGA			
1	Information security and service management	Has the manufacturer of DiGA implemented an information security management system (ISMS) in accordance with ISO/IEC 27001 or in accordance with ISO/IEC 27001 on the basis of IT basic protection (BSI-Standard 200-2: IT Basic Protection Methodology) and can – from April 1, 2022 – present a corresponding, recognized certificate at the request of BfArM?	
2	Information security and service management	Does the manufacturer of DiGA have a structured protection requirement analysis, taking into account the damage scenarios "violation of laws/ regulations/contracts," "impairment of the right to informational self-determination," "impairment of personal integrity," "impairment of task performance," and "negative internal or external effects" carried out and documented, which leads to a normal, high or very high protection requirement according to the definition of the BSI-Standard 200-2 for DiGA, and can the manufacturer of DiGA submit the documentation of the protection requirement analysis at the request of BfArM?	
3	Information security and service management	Has the manufacturer of DiGA implemented and documented processes of release, change, and configuration management, taking into account the requirements of Regulation (EU) 2017/745, which ensure that extensions and adjustments to DiGA that the manufacturer developed themselves or on behalf of another organization have been adequately tested and explicitly approved before it goes into production?	

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

4	Prevention of data leakage	Has the manufacturer of DiGA ensured that the communication of DiGA with other services is technically restricted to such an extent that no unwanted data communication, via which personal data can be sent, is possible?	
5	Prevention of data leakage	Is at least one transport encryption in accordance with the minimum standard of the BSI for the use of Transport Layer Security (TLS) according to Section 8 Paragraph 1 Sentence 1 of the BSI law used for every data communication between different system components of DiGA that takes place via open networks?	DiGA does not trigger any data communication that takes place over open networks.
6	Prevention of data leakage	Whenever functionalities of DiGA that can be accessed via the Internet are accessed, does DiGA check the authenticity of the services before personal data are exchanged with them?	DiGA does not have any functionality that can be accessed via the Internet.
7	Prevention of data leakage	Has the manufacturer of DiGA ensured that DiGA does not write any unwanted log or auxiliary files?	
8	Prevention of data leakage	Has the manufacturer of DiGA ensured that DiGA does not send error messages that may reveal confidential information?	
9	Authentication	Do all persons using DiGA authenticate themselves via a method that is appropriate to the protection requirements for the data processed by DiGA before data accessible via DiGA can be accessed?	
10	Authentication	Are suitable technical measures applied to ensure that the data used to authenticate a person who uses DiGA is never exchanged via unsecured transport connections?	

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

11	Authentication	Does DiGA use or contain a central authentication component that was implemented with established standard components, which is only permitted for the initial authentication and whose trustworthiness can be verified by the services of DiGA?	
12	Authentication	Does DiGA enforce that a person using DiGA can only change the data used for their authentication if doing so includes sufficient information to verify the authenticity of that person?	
13	Authentication	If authentication takes place using a password: –does DiGA force everyone who uses DiGA to set strong passwords in accordance with a password policy that includes a minimum password length and limits for failed login attempts? –is it ensured that passwords are never transmitted or stored in plain text? –are password changes or resets logged, and is the data subject informed immediately about the password reset or change, provided suitable contact information is available?	Authentication is not carried out via a password.
14	Authentication	If DiGA stores authentication data on an end device or in a software component, is the explicit consent of the person using DiGA requested ("opt-in"), and is the user informed of the risks of the function?	DiGA does not store any authentication data on a device or in a software component.

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

15	Authentication	If the information on the identity or authenticity of the person using DiGA or on the authenticity of components of DiGA is shared between components of DiGA via dedicated sessions (“Sessions”): –are all session data, both during exchange and storage, protected with technical measures that are appropriate to the protection requirements of DiGA, and are any session IDs used generated randomly, with sufficient entropy, and using established procedures? –are all sessions established in an instance of DiGA invalidated when the use of DiGA is canceled or terminated? –can the person using DiGA also force a session to be explicitly invalidated? –do sessions have a maximum validity period, and are inactive or interrupted sessions automatically invalidated after a certain period of time? –does the invalidation of a session result in the deletion of all session data, and is it ensured that a session that has become invalid cannot be reactivated even if individual session data is known?	DiGA does not use sessions.
16	Authentication	Can DiGA support authentication of GKV-insured persons as the persons using DiGA via the secure digital identity according to Section 291 Paragraph 8 of Book V of the Social Code by 1 January 2024, at the latest?	
17	Access control	Does DiGA ensure that every access to protected data and functions undergoes an authorization check ("complete mediation"), for which a dedicated authorization component including all protected data is used for access by operating personnel of the manufacturer of DiGA ("reference monitor “ or “secure node/application”), which requires prior secure authentication of the accessing person?	

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

18	Access control	Are all authorizations initially and restrictively assigned by default, and can authorizations only be extended via controlled procedures that include effective verification and control mechanisms based on a multiple-eyes principle when authorizations for operating personnel of the manufacturer of DiGA change?	
19	Access control	If DiGA provides for different user roles, can each role only access functions of DiGA with the rights required to perform the functionalities associated with the role?	The digital health application does not provide for different user roles.
20	Access control	Does the manufacturer of DiGA ensure that access to functions and data of DiGA by the manufacturer's operating personnel is only possible via secure networks and access points?	
21	Access control	Do all access control errors and malfunctions result in denial of access?	
22	Incorporating data and functions	Can the insured person move exclusively within the trust domain of DiGA, or can only trustworthy external content checked by the manufacturer of DiGA be used with DiGA, and will the insured person be informed if the trust domain of DiGA is left?	
23	Incorporating data and functions	If DiGA allows the user to upload files, is this function restricted as much as possible (e.g., excludes active content), is the content checked for security, and is it ensured that files can only be saved in the specified path?	DiGA does not allow uploading files.
24	Logging	Does DiGA carry out a complete, traceable, tamper-proof logging of all security-related events – i.e. those relating to the secure identification, authentication, and authorization of people and organizations?	

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

25	Logging	Is logging data evaluated automatically in order to identify or proactively prevent security-related events?	
26	Logging	Is access to logging data secured by appropriate authorization management and restricted to a few authorized persons and defined purposes?	
27	Regular and secure updates	Does the manufacturer of DiGA inform the data subject (e.g., via push notifications or before DiGA is launched) if a security-relevant update of DiGA has been made available for installation or carried out?	
28	Safe uninstall	If DiGA is uninstalled, will all data and files created by the DiGA – including caches and temporary files – and stored on IT systems at the disposal of the data subject be deleted?	DiGA is a purely web-based app.
29	Hardening	If services of DiGA can be accessed via web protocols: –are methods of the protocols used that are not required deactivated for all services that can be accessed via open networks? –are the allowed character encodings restricted as much as possible? –are access attempt limits set for all services accessible over open networks? –is it ensured that no security-related comments or product and version information are disclosed? –are unnecessary files regularly deleted? –is it ensured that these services are not recorded by search engines? –are absolute local path specifications omitted? –is retrieval of source texts excluded?	DiGA does not include any services accessible via web protocols.

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

30	Hardening	If DiGA processes data provided by the user or sources that are not controlled by DiGA: –is this data treated as potentially dangerous and appropriately validated and filtered? –is this data checked on a trustworthy IT system? –are incorrect entries not processed automatically, or are the corresponding functionalities implemented securely so that misuse is ruled out? –is this data encoded in a form that ensures malicious code is not interpreted or executed? –is this data separated from specific requests to data-holding systems (e.g., via stored procedures), or are data requests explicitly secured against attack vectors favored by such data?	DiGA does not process data provided by the user or sources that are not controlled by DiGA.
31	Hardening	Is it consistently ensured that errors in DiGA are handled and lead to the termination and, if necessary, rollback of the initiated functions?	
32	Hardening	Is DiGA protected against automated access with suitable protective mechanisms if these do not realize the intended uses of DiGA?	
33	Hardening	Are configuration files relevant for the secure operation of DiGA protected against loss and falsification with appropriate technical measures?	DiGA does not use any configuration files or files that are not relevant to the secure operation of DiGA.
34	Penetration testing	Has the manufacturer of DiGA carried out a penetration test for the version of DiGA to be included in the directory pursuant to Section 139e Paragraph 1 of Book V of the Social Code – including all back-end components – which follows the implementation concept for penetration tests recommended by the Federal Office for Information Security, and – as far as the applicability is given – also takes into account the current OWASP top 10 security risks? Can the manufacturer of DiGA submit corresponding evidence for the implementation of the penetration tests and elimination of the vulnerabilities found?	

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

35	Useof sensors and external devices	If DiGA directly accesses sensors on a mobile device and/or external hardware (e.g., sensors close to the body): –has the manufacturer of DiGA specified the general conditions under which sensors or connected devices can be installed, activated, configured, and used, and is the existence of these general conditions ensured as much as possible before the corresponding functionalities are executed? –does DiGA ensure that sensors and connected devices are defaulted to a documented security policy upon installation or initial activation for DiGA? –can the insured person reset sensors and devices directly controlled by DiGA to a default setting that conforms to a documented security policy? –is data exchange between DiGA and directly controlled sensors or devices only possible once the installation and configuration of the sensors or devices are fully completed?	The digital health application does not access the sensors of a mobile device or external hardware.
36	Useof sensors and external devices	If DiGA exchanges data with external hardware (e.g., sensors close to the body): –are the procedures for installing, configuring, activating, and deactivating this hardware described in a way that is appropriate for the target group, and is it secured against operating errors as much as possible? –is there mutual authentication between DiGA and external hardware? –is data exchanged between DiGA and external hardware only encrypted after an initial handshake? –is it ensured that all data stored on external hardware is deleted when DiGA is uninstalled or terminated? –has the manufacturer of DiGA documented how connected hardware can be safely deactivated so that no data is lost and no sensitive data remains on the device?	DiGA does not exchange data with external hardware.
37	Use of third-party software	Does the manufacturer of DiGA keep a complete list of all libraries and other software products used in DiGA that were not developed by the manufacturer of DiGA?	
38	Use of third-party software	Does the manufacturer of DiGA use suitable market observation procedures to ensure that previously unknown risks to data protection, data security, or patient safety emanating from these libraries or products are identified promptly?	

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

39	Use of third-party software	Has the manufacturer of DiGA established procedures to take appropriate measures in the event of such identified risks to be able to immediately block the app and notify users?	

Additional requirements for DiGA for the highest level of protection

1	Encryption of stored data	Are personal data processed on IT systems that are not at the personal disposal of the user only stored in encrypted form on these systems?	
2	(omitted)		
3	(omitted)		
4	Authentication	Is two-factor authentication enforced, at least for the initial authentication of all people using DiGA?	
5	Authentication	If DiGA allows for a fallback option to one-factor authentication: –is the person using DiGA informed about the associated risks, and is such a relapse only activated after the user has given their consent, confirmed by an active action? –can the person using DiGA deactivate this fallback option at any time?	DiGA does not allow for a fallback option to one-factor authentication.
6	(omitted)		
7	Authentication	If DiGA provides for a user role for service providers, can the DiGA support authentication of service providers as the persons using DiGA via an electronic health professional card with a contactless interface by 31 December 2020, at the latest?	DiGA is not intended for use by service providers.
8	Measures against DoS and DDoS	Are messages (XML, JSON, etc.) and data sent to DiGA services accessible via open networks checked against defined schemes?	DiGA does not exchange data with or between services accessible via open networks.

Appendix 1 – DiGA Compliance Checklist: Data Protection and Data Security

9	Embedded web servers	If the components belonging to DiGA are web servers: –is the web server configured as restrictively as possible? –are only the required components and functions of the web server installed or activated? –if possible, is the web server not operated under a privileged account? –are security-related events logged? –is access only possible after authentication? –is all communication with the web server encrypted?	DiGA does not use a web server.

Appendix 2 – DiGA Compliance Checklist: Quality and Interoperability

Using the questionnaire listed below, the manufacturer must declare compliance with the requirements for quality and interoperability. Compliance with a requirement is confirmed by marking it in the "Applicable" column or, if the justification given there applies, in the "Not applicable" column.

No.	DiGAV reference	Requirement	Applicable / Not applicable	Acceptable justification for “Not applicable”
Interoperability				
Can the insured person export the data processed via DiGA from DiGA in an interoperable format?				
1	Section 5 Paragraph 1 and Section 6	Yes, the data processed via DiGA can be exported by the insured person from DiGA in an interoperable format (syntax and semantics) and made available to the insured person for further use. The transmission, according to Sentence 1, is carried out according to a definition for the semantic and syntactic interoperability of data in the electronic patient file according to Section 355 Paragraph 2a of Book V of the Social Code. As long as there is no such definition, the transmission is carried out according to an open, recognized international standard or a profile disclosed by the manufacturer of DiGA via an open, recognized international standard.		
Can the insured person export the data processed via DiGA from DiGA in a form that can be used for care?				
2	Section 5 Paragraph 1 and Section 6	Yes, the insured person can export from DiGA relevant excerpts of the health data processed via DiGA, in particular, in the course of therapy, therapy planning, therapy results, and data evaluations. The export is conducted in a human-readable and printable format, with the healthcare context in which DiGA is typically used according to its intended purpose taken into account.		

Appendix 2 – DiGA Compliance Checklist: Quality and Interoperability

Does DiGA have standardized interfaces for personal medical devices?			
3	Section 5 Paragraph 1 and Section 6	Yes, DiGA is able to collect data from medical devices or wearable sensors for measuring and transmitting vital signs (wearables) used by the insured person and supports a disclosed and documented profile of the ISO/IEEE 11073 standard. If such a suitable profile is not available, DiGA supports another disclosed and documented interface (syntax, semantics) that is recommended in the interoperability directory according to Section 385 of Book V of the Social Code. If such a suitable interface does not exist, DiGA supports another disclosed and documented interface.	DiGA is not intended to exchange data with medical devices used by the insured person or with sensors worn by the insured person for measuring and transmitting vital signs (wearables).
Are the standards and profiles used to ensure the interoperability of DiGA published? Are they used without discrimination?			
4	Section 5 Paragraph 1 and Section 6	Yes, the standards and profiles used to ensure the interoperability of DiGA are fully published, linked on the application website, used in a non-discriminatory manner, and can be implemented by third parties in their systems.	
4a	Section 6	Yes, if the manufacturer of DiGA has their own profiles, they are published in a recognized directory.	The manufacturer of DiGA doesn't have their own profiles.
Does DiGA offer the insured person suitable options for data transfer to the electronic patient file?			
5	Section 6a	Yes, DiGA allows the insured person to transfer the data processed by DiGA to their electronic health record at any time, upon their consent, from 1 January 2024. In addition, DiGA offers the user the option of regular, automated transmission of the data processed by DiGA from DiGA to the electronic patient file. The manufacturer of DiGA has enabled the user to configure the regular automated transmission in a way that is adapted to the intended use of DiGA and the supply context. The manufacturer transfers the data to the electronic patient file.	

Appendix 2 – DiGA Compliance Checklist: Quality and Interoperability

Robustness			
Is DiGA robust against disruptions and operating errors?			
1	Section 5 Paragraph 2	Yes – a sudden power failure will not result in data loss.	
2	Section 5 Paragraph 2	Yes – a sudden Internet failure will not result in a loss of data.	
3	Section 5 Paragraph 2	Yes, DiGA checks the plausibility of measurements, inputs, and other data from external sources.	DiGA is not able to collect data from medical devices or sensors or from other external sources, nor does it provide for the input of data.
4	Section 5 Paragraph 2	Yes, DiGA includes functions for testing and/or calibrating connected medical devices and sensors.	DiGA is not able to collect data from medical devices or sensors.
Consumer protection			
Does the user of DiGA receive all the information they need to make a usage decision before making any commitments to the manufacturer or a third party?			
1	Section 5 Paragraph 3	Yes, the range of functions is fully described in the information about DiGA on the sales platform and the app website, and the medical purpose is fully explained.	
2	Section 5 Paragraph 3	Yes, the information about DiGA on the sales platform and the app website clearly shows what features are available with the download or use of the app and what features are available after purchasing and at what price, as in-app purchases or function forwarding can or must be made.	
Is the compatibility of DiGA with systems and devices communicated transparently?			
3	Section 5 Paragraph 3	Yes, the manufacturer of DiGA has published a list of compatibility promises regarding operating system versions and mobile devices or web browsers and web browser versions, as well as other required or optional devices on the app website and keeps this list up to date.	

Appendix 2 – DiGA Compliance Checklist: Quality and Interoperability

Has the manufacturer published the medical purpose of DiGA?			
4	Section 5 Paragraph 3	Yes, the medical purpose is published in the imprint of DiGA according to Article 2 Number 12 of Regulation (EU) 2017/745 and Section 3 Number 10 of the Medical Devices Act in the version valid up to and including 25 May 2020.	
Are the terms of use of DiGA designed to be consumer-friendly?			
5	Section 5 Paragraph 4	Yes, DiGA is ad-free.	
6	Section 5 Paragraph 3	Yes, DiGA only contains transparent offers, such as automatically renewing subscriptions or time-limited special offers.	
7	Section 5 Paragraph 3	Yes, DiGA contains measures to protect against unintentional in-app purchases or does not offer in-app purchases.	
Does the manufacturer of DiGA implement measures to support users?			
8	Section 5 Paragraph 5	Yes, the manufacturer provides free support in the German language to help users run DiGA, which answers user inquiries within 24 hours at the latest.	
Ease of use and accessibility			
Is DiGA easy-to-use and intuitive?			
1	Section 5 Paragraph 5	Yes, the usability style guides of the respective platform for mobile apps have been fully implemented, or alternative solutions, the user-friendliness of which have been proven by user tests, have been implemented.	DiGA is not used on mobile devices.
2	Section 5 Paragraph 5	Yes, the easy and intuitive usability of DiGA is confirmed by tests with focus groups representing the target group.	
3	Section 5 Paragraph 6	Yes, DiGA offers accessibility features for people with disabilities or supports the accessibility features offered by the platform.	

Appendix 2 – DiGA Compliance Checklist: Quality and Interoperability

Support of service providers			
Does DiGA inform and support doctors and other service providers involved in its use?			
1	Section 5 Paragraph 7	Yes, the manufacturer of DiGA provides information for integrated healthcare providers, which describes in an understandable way the additional use of the app by a healthcare provider and the underlying roles of healthcare providers and patients.	No involvement of service providers is planned for the use of DiGA.
2	Section 5 Paragraph 7	Yes, the manufacturer of DiGA provides information for involved care providers, which describes how the use of DiGA can be explained to the insured person as part of the therapy.	No involvement of service providers is planned for the use of DiGA.
3	Section 5 Paragraph 7	Yes, the user can activate their data access for service providers to be involved or transmit data securely to service providers.	No involvement of service providers is planned for the use of DiGA.
Quality of medical content			
Is DiGA based on reliable medical knowledge? Is DiGA transparent?			
1	Section 5 Paragraph 8	Yes, the medical content and procedures implemented in DiGA are based on the generally recognized professional standard.	
2	Section 5 Paragraph 5	Yes, the manufacturer has established suitable processes to keep the medical content and procedures implemented in DiGA up to date.	
3	Section 5 Paragraph 8	Yes, the sources for the medical content and procedures implemented in DiGA – such as guidelines, textbooks, and studies – are published and named in DiGA or on a website linked from DiGA.	
4	Section 5 Paragraph 8	Yes, the studies conducted with DiGA are published and named in DiGA or on a website linked from DiGA.	

Appendix 2 – DiGA Compliance Checklist: Quality and Interoperability

	Is the health information with which DiGA supports the user appropriate?		
5	Section 5 Paragraph 8	Yes, the health information offered in DiGA is up-to-date and based on generally recognized professional standards.	DiGA does not offer health information.
6	Section 5 Paragraph 8	Yes, the manufacturer has established suitable processes to keep the health information offered in DiGA up to date.	
7	Section 5 Paragraph 8	Yes, the sources for the health information offered in the DiGA are published and named in DiGA or on a website linked from DiGA.	DiGA does not offer health information.
8	Section 5 Paragraph 8	Yes, the health information provided in DiGA is adapted to the target group.	DiGA does not offer health information.
9	Section 5 Paragraph 8	Yes, the health information is provided on a case-by-case basis and in the context of the respective use of DiGA.	DiGA does not offer health information.
10	Section 5 Paragraph 8	Yes, in DiGA, didactic processes are implemented to deepen and strengthen the health knowledge offered.	DiGA does not offer health information.
	Patient safety		
	Does the manufacturer implement appropriate measures to improve patient safety?		
1	Section 5 Paragraph 9	Yes – on the sales platform or before the launch of DiGA, the manufacturer clearly states for what patients and indications DiGA should not be used, provided there are restrictions.	
2	Section 5 Paragraph 9	Yes, DiGA gives the user context-sensitive information about risks and about suitable measures to mitigate or avoid them.	
3	Section 5 Paragraph 9	Yes, in the context of critical measured values or analysis results, DiGA clearly indicates the necessity or the usefulness of consultation with a doctor or another service provider.	

Appendix 2 – DiGA Compliance Checklist: Quality and Interoperability

4	Section 5 Paragraph 9	Yes, DiGA recommends that the user cease the use of DiGA or change the way of using DiGA if a defined condition is determined.
5	Section 5 Paragraph 9	Yes, for all values entered by the user or collected via the connected medical devices or sensors or taken from other external sources, consistency conditions are defined in DiGA, which are checked before a value is used.
6	Section 5 Paragraph 9	Yes, error messages are designed in DiGA in such a way that the user can understand where the error was and how they can avoid it in the future.

Appendix 3 – List of Deliverables

Process	Reference standard	Deliverable (Technical Documentation)
Project management	ISO 13485	Project Management Plan Quality Agreement
Software development	IEC 62304, IEC 82304-1, ISO 13485	Software Development Plan Traceability Analysis
Software description	IEC 62304, IEC 82304-1, ISO 13485	Software Requirements Specification Software Specification Review
Software design	IEC 62304, IEC 82304-1, ISO 13485	Software Architecture Document
Software testing	IEC 62304, IEC 82304-1, ISO 13485	Test Plan Test Cases Test Report
Software security testing	IEC 82304-1, IEC 81001-5-1, DiGAV IEC 82304-1, IEC 81001-5-1, DiGAV	Security Test Plan Security Test Report
Software acceptance and handover	IEC 62304, IEC 82304-1	Release Notes
Product risk management	ISO 14971 ISO 14971, ISO/IEC 27001, IEC 81001-5-1	Risk Management File IT Security Risk Assessment
Usability	IEC 62366	Usability Engineering File
Clinical evaluation	MDR	Clinical Evaluation Plan (Performance Test Plan) Clinical Evaluation Report (Performance Test Report)
Change and configuration management	IEC 62304, IEC 82304-1, ISO 13485, IEC 81001-5-1	Configuration and Change Management Plan
Document management	ISO 13485	Document Management Plan
Regulatory	MDR	Technical File

Appendix 3 – List of Deliverables

Software maintenance	IEC 62304, IEC 82304-1, ISO 13485	Software Maintenance Plan IFU/Manual
UDI	MDR	UDI & Label
Design review	ISO 13485	Technical File Review Report
QMS/ISMS standard operating procedures		
QMS/ISMS	ISO 13485ISO/IEC 27001	Quality Management Manual
QMS/ISMS	ISO 13485ISO/IEC 27001	Quality objectives (including IS)
QMS/ISMS	ISO 13485ISO/IEC 27001	Organizational Chart, Definition of Roles
QMS/ISMS	ISO 13485ISO/IEC 27001	SOP Management Review/SOP Performance Measurement
QMS/ISMS	ISO 13485ISO/IEC 27001	SOP Data Analysis/SOP Performance Measurement
QMS/ISMS	ISO 13485ISO/IEC 27001	SOP Control of Documents and Records
QMS/ISMS	ISO 13485ISO/IEC 27001	SOP CAPA (including ISMS)
QMS	ISO 13485ISO/IEC 27001	SOP Internal and External Audits
QMS	ISO 13485	SOP Reporting of Incidents and Recalls EU
QMS	ISO 13485	SOP Computer System Validation
QMS	ISO 13485	SOP Recruiting and Training
IQMS	ISO 13485	SOP Purchasing and Supplier Management
QMS	ISO 13485	SOP Software Development
QMS	ISO 13485	SOP Support, Feedback Handling, Complaint Handling
ISMS	ISO/IEC 27001	Information Security Guideline
ISMS	ISO/IEC 27001	Information Security Policy

Appendix 3 – List of Deliverables

ISMS	ISO/IEC 27001	IS Risk management Policy
ISMS	ISO/IEC 27001	Risk Registry
ISMS	ISO/IEC 27001	Asset Registry
ISMS	ISO/IEC 27001	Information Security Incident Management Policy
ISMS	ISO/IEC 27001	Mobile Device Policy
ISMS	ISO/IEC 27001	Asset Management Policy
ISMS	ISO/IEC 27001	Information Classification Policy
ISMS	ISO/IEC 27001	Access Control Policy
ISMS	ISO/IEC 27001	Encryption Management Policy
ISMS	ISO/IEC 27001	Physical and Environmental Security Policy
ISMS	ISO/IEC 27001	Operations Security Policy
ISMS	ISO/IEC 27001	Backup and Restore Policy
ISMS	ISO/IEC 27001	Vulnerability Management Policy
ISMS	ISO/IEC 27001	Communication Policy
ISMS	ISO/IEC 27001	Business Continuity Management Policy

Appendix 4 – Training Required

Training title	Training description
ISO 13485 for Medical Devices: Quality Management Systems (QMS)	Training on the requirements of the ISO 13485 standard.
QMS: Introduction	Training on QMS Standard Operating procedures.
EN ISO 14971: Application of Risk Management to Medical Devices	Training on the requirements of the ISO 14971 standard.
IEC 62304: Software Development Life Cycle	Training on the requirements of the IEC 62304 standard.
IEC 62366 for Medical Devices, Part 1: Application of Usability Engineering to Medical Devices	Training on the requirements of the IEC 62366 standard.
ISO/IEC 27001: Information Security, Cyber Security, and Privacy Protection, Information Security Management Systems (ISMS), Requirements	Training on the requirements of the ISO/IEC 27001 standard.
ISMS: Introduction	Training on ISMS Policies.