Ordinance Governing Procedures and Requirements in Determining the Reimbursability of Digital Health Applications in Statutory Health Insurance (Digital Health Applications Ordinance – DiGAV)

2020

On the basis of Sections 134 (3) sentence 17 and 139e (7)-(9) of the Social Code Book (*Sozialgesetzbuch - SGB*) V ("SGB V"), which were inserted by way of Art. 1 No. 23 of the Act of 9 December 2019 (Federal Law Gazette I p. 2562), the Federal Ministry of Health decrees as follows:

Section 1

Eligibility and application details

§ 1
Eligibility

(1) The procedure for adding digital health applications to the directory of digital health applications of the Federal Institute for Drugs and Medical Devices (*Bundesinstitut für Arzneimittel und Medizinprodukte - BfArM*) pursuant to Section 139e (1) SGB V is instituted upon the manufacturer's request.

(2) The manufacturer within the meaning of this ordinance is the maker of the medical device within the meaning of applicable provisions under medical device law.

(3) If a third party files an application on a manufacturer's behalf, such party must attach a written power of attorney from the manufacturer to the application in either written or electronic form. Otherwise, third parties are not authorized to file applications.

§ 2
Application details

(1) The application to be filed with the Federal Institute for Drugs and Medical Devices by the manufacturer of a digital health application contains information about the requirements under Section 139e (2) sentence 2 SGB V. In addition, the application includes but is not limited to details about:

1. the manufacturer as well as the digital health application's defining characteristics;
2. the intended medical purpose pursuant to applicable provisions under medical device law;
3. the notified body involved in the conformity assessment procedure pursuant to applicable provisions under medical device law, as applicable;
4. the user manual pursuant to applicable provisions under medical device law;
5. the intended effect, mode of action, contents and use of the digital health application in layman's terms;
6. the functions of the digital health application;
7. the medical institutes and organizations involved in the development of the digital health application, if applicable;
8. the sources for the medical content and processes implemented in the digital health application, including but not limited to guidelines, textbooks, and studies;
9. any available or intended evidence of positive healthcare effects pursuant to §§ 8 and 9 in layman's terms – summarized in keeping with the PICO process;
10. any patient group for which positive healthcare effects have been substantiated pursuant to §§ 8 and 9 or, in the event of provisional listing, are to be proven during the trial period;
11. any positive healthcare effect that has been substantiated for the stated patient group pursuant to §§ 8 and 9 or, in the event of provisional listing, is to be proven during the trial period, as broken down into proof of medical benefits and proof of patient-relevant improvements of structure and processes in patient care;
12. the study or studies submitted by the manufacturer to substantiate positive healthcare effects pursuant to §§ 10 and 11 or, if applicable, such systematic data analysis as the manufacturer may provide to establish positive healthcare effects pursuant to § 14;
13. the study undertaken to establish the test accuracy of the diagnostic instruments employed by the digital health application pursuant to § 12, if applicable;
14. the institution that is independent from the manufacturer pursuant to Section 139e (4) SGB V, if applicable;
15. satisfying the requirements of §§ 3-6;
16. the user roles for which the digital health application provides;
17. the quality-assured use of the digital health application, including but not limited to the exclusion criteria for use;
18. the actions that the manufacturer deems necessary on the part of statutory health insurance-accredited physicians for the use of the digital health application, if applicable;
19. the minimum period of use of the digital health application that the manufacturer deems necessary;
20. the sites where data is processed for the digital health application;
21. the compatibility assurances of the manufacturer of the digital health application in reference to supported platforms and devices, along with any additional products needed;
22. the standards and profiles used to bring about the semantic and technical interoperability of the digital health application;

23. the amount of coverage available under the manufacturer's liability insurance policy for personal injury claims; and

24. the actual rates pursuant to Section 134 (5) sentence 1 SGB V.

(2) In its application, the manufacturer marks any entry under paragraph 1 for which publication is opposed by legal requirements pertaining to the protection of business or trade secrets or the protection of personal data or intellectual property.

(3) The manufacturer indicates in the application whether it seeks final listing in the directory of digital health applications pursuant to Section 139e (2) SGB V or provisional listing for trial purposes pursuant to Section 139e (4) SGB V.

(4) The manufacturer provides the Federal Institute for Drugs and Medical Devices with free access to the digital health application in the application.

Section 2

Requirements as to safety, functionality, data protection and security as well as the quality of digital health applications

§ 3
Requirements as to safety and functionality

(1) Subject to paragraph 2, the CE conformity marking of the medical device is recognized as proof of safety and functionality as a rule.

(2) Subject to justified cause, the Federal Institute for Drugs and Medical Devices may undertake additional reviews. For this purpose, it may call on the manufacturer of the digital health application to submit any required documentation, including but not limited to the declarations and certificates needed for the conformity assessment procedure.

§ 4
Requirements as to data protection and security

(1) Digital health applications must conform to statutory data protection provisions as well as the requirements concerning data security according to the state of the art, and account for the nature of data processed, relevant protection levels and the need for protection.

(2) In the context of digital health applications, personal data may be processed only with the consent of the insured pursuant to Art. 9(2) point 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) (Official Journal L 119 of 4 May 2016, p. 1), and only for the following purposes:

1. to have users put the digital health application to its intended use;

2. to substantiate positive healthcare effects as part of a trial pursuant to Section 139e (4) SGB V;

3. to offer proof in the context of agreements pursuant to Section 134 (1) sentence 3 SGB V; and

4. to permanently ensure the digital health application's technical functionality, user friendliness and ongoing improvement. The consent of the insured to data processing pursuant to sentence 1 number 4 is to be obtained separately from their consent to data processing for purposes of sentence 1 numbers 1-3. This shall be without prejudice to such authority to process data as may be conveyed by other provisions.

(3) As part of a digital health application, the processing of personal data by the digital health application itself as well as any processing of personal data on behalf of a controller must take place in Germany, in a member state of the European Union or in such country as may be equivalent thereto pursuant to Section 35 (7) Social Code Book I or, in the event that an adequacy decision has qualified a third country pursuant to Art. 45 of Regulation (EU) 2016/679, in such third country.

(4) Personal data must not be processed for purposes other than those stated in paragraph 2 sentence 1, including but not limited to marketing purposes. This shall be without prejudice to such authority to process data as may be conveyed by other provisions according to paragraph 2 sentence 3.

(5) The manufacturer of digital health applications imposes a duty of confidentiality on all individuals working on its behalf, who have access to the personal data of the insured.

(6) Annex 1 provides details on the requirements according to the foregoing paragraphs. The manufacturer attaches the declaration according to Annex 1 to its application. In the event that the requirements of Annex 1 with regard to the characteristics of the digital health application prove unsuitable, the digital health application may deviate from the requirements of Annex 1 on a case-by-case basis if statutory data protection provisions as well as the requirements concerning data security according to the state of the art are implemented equally by other means of implementation. The manufacturer addresses, and explains, any instance of deviation from the provisions of Annex 1 in its application.

§ 5
Requirements as to quality

(1) Digital health applications are to be designed to implement the requirements as to semantic and technical interoperability. Specifically, the digital health application must allow data processed by it to be exported in suitable interoperable formats and used as part of healthcare delivery. In addition, the digital health application must use interoperable interfaces if it is envisioned as part of the intended use of the digital health application that it exchanges data with medical devices used by the insured or such sensors as the insured may wear to measure and transmit vital sign values ("wearables").

(2) Digital health applications are to be designed to withstand malfunctions and operating errors.

(3) Digital health applications are to be designed to implement the requirements of consumer protection under Annex 2. Specifically, the digital health application must provide the insured with information on its scope of functionality and intended use, along with the contractual terms of use, prior to the commencement of use.

(4) Digital health applications must be free from advertising.

(5) Digital health applications are to be designed to allow the insured to operate them easily and intuitively. While they are listed in the official directory of digital health applications and for the duration of their use at the expense of the statutory health insurance funds pursuant to Section 33a (1) SGB V, at a minimum, digital health applications must provide for measures intended to support the insured.

(6) Digital health applications implement the requirements concerning accessibility in accordance with Annex 2.

(7) If it is necessary for purposes of the intended use of a digital health application to involve healthcare providers in the application's use, the application must ensure that the healthcare providers are appropriately informed and supported.

(8) The medical contents on which digital health applications rely must reflect the generally recognized state of medical knowledge. Insofar as the digital health application supports the insured by delivering health information, such information must likewise reflect the generally recognized professional standards of the field and be communicated with an eye toward the target audience.

(9) Digital health applications must provide for measures designed to promote patient safety.

(10) Annex 2 provides details on the requirements according to the foregoing paragraphs. In the event that the requirements of Annex 2 with regard to the characteristics of the digital health application prove unsuitable, the digital health application may deviate from the requirements of Annex 2 on a case-by-case basis if the requirements are equally satisfied by other means of implementation. The manufacturer addresses, and explains, any instance of deviation from the provisions of Annex 2 in its application.

(11) The manufacturer encloses with its application a declaration according to Annex 2.

§ 6

Quality requirements pursuant to § 5 para. 1; determinations regarding interoperability

All specifications regarding the contents of electronic patient records pursuant to Section 291b (1) sentence 7 SGB V as well as the standards and profiles recommended in the directory pursuant to Section 291e SGB V are deemed interoperable within the meaning of § 5 para. 1. If there is no suitable determination pursuant to Section 291b (1) sentence 7 SGB V, and no suitable determination as to interoperability that has been designated "recommended" is found in the directory pursuant to Section 291e SGB V, then open, internationally recognized interface and semantic standards as well as such profiles as the manufacturer of the digital health application may provide for open, internationally recognized interface and semantic standards or standards registered in the directory pursuant to Section 291e SGB V, too, are deemed interoperable. The manufacturer must publish profiles provided under sentence 2 free of charge for public use and request that they be included in the directory pursuant to Section 291e SGB V.

§ 7

Proof by certificates

(1) The Federal Institute for Drugs and Medical Devices may call on the manufacturer to submit certificates to confirm the satisfaction of the requirements of §§ 4-6 as far as such certificates are indicated on the basis of safety, quality or environmental standards or other recognized certificates are capable of establishing compliance with the requirements of §§ 4-6. The certificate to be submitted pursuant to sentence 1 must not be older than twelve months at the time of its transmission to the Federal Institute for Drugs and Medical Devices. As a rule, evidence of the satisfaction of the requirements of §§ 4-6 is deemed to have been furnished once such a certificate has been submitted. § 3 para. 2 applies accordingly.

(2) Proof pursuant to paragraph 1 entails the submission of a certificate issued by an accredited certification body authorized to do so in accordance with the provisions of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 of the Council (Official Journal L 218 of 13 August 2008, p. 30). The certification body must further be accredited and authorized under Section 39 of the Federal Data Protection Act (*Bundesdatenschutzgesetz - BDSG*) to issue certifications pursuant to § 4. The Federal Institute for Drugs and Medical Devices may announce on its webpages which certificates are capable of establishing compliance with the requirements of §§ 4-6.

(3) Specifically, the Federal Institute for Drugs and Medical Devices may call on the manufacturer of the digital health application to submit suitable certificates or evidence with a view to establishing compliance with the requirements as to information security starting no later than 1 January 2022.

Section 3

Requirements for substantiating positive healthcare effects

§ 8

Meaning/Definition of positive healthcare effects

(1) Within the meaning of this ordinance, positive healthcare effect refers to either a medical benefit or patient-relevant improvements of structure and processes in patient care.

(2) Within the meaning of this ordinance, medical benefit refers to the patient-relevant effect, especially with regard to improving patient health, shortening the length of an illness, prolonging survival time or improving quality of life.

(3) Within the meaning of this ordinance, patient-relevant improvements of structure and processes in patient care as part of detecting, monitoring, treating or alleviating illnesses or detecting, treating, alleviating or compensating for injuries or disabilities are geared toward supporting the health behavior of patients or integrating the processes between patients and healthcare providers and specifically encompass the areas of:

1. coordinating treatment procedures;
2. aligning treatment with guidelines and recognized standards;
3. adherence;
4. facilitating access to patient care;
5. patient safety;
6. health literacy;
7. patient autonomy;
8. coping with illness-related difficulties in everyday life; or
9. reducing therapy-related efforts and strains for patients and their relatives.

§ 9

Detailing positive healthcare effects

(1) In its application for listing in the directory of digital health applications pursuant to § 2, the manufacturer states:

1. the nature of the positive healthcare effects offered by the digital health application that are to be substantiated; and
2. the patient group for which the positive healthcare effects under sentence 1 are to be substantiated.

(2) The positive healthcare effects postulated by the manufacturer pursuant to paragraph 1 number 1 must be consistent with the intended use pursuant to applicable provisions under medical device law, along with the functions and contents of as well as such public pronouncements as the manufacturer may make about the digital health application.

(3) To identify the relevant patient group pursuant to paragraph 1 number 2, the manufacturer provides one or more indications pursuant to IDC-10-GM – in most cases, a three-digit code. If no patient group can be defined in accordance with sentence 1 using a three-digit code, the manufacturer may provide one or more indications pursuant to ICD-10-GM using four digits. In the event that the manufacturer provides several indications, it may, as a rule, furnish proof pursuant to paragraph 1 number 2 for all indications combined, provided that such indications are essentially comparable in terms of the positive healthcare effect to be substantiated. If this is not the case, the manufacturer must furnish proof separately for each given indication. Explanations are to be supplied for any definition pursuant to sentence 2 as well as for the comparability of indications pursuant to sentence 3.

§ 10

Studies substantiating positive healthcare effects

(1) As evidence of the positive healthcare effects claimed in accordance with § 9 para. 1, the manufacturer submits a comparative study showing that using the digital health application is better than not using it. Comparative studies within the meaning of sentence 1 are retrospectively comparative studies, including retrospective studies featuring an intra-individual comparison.

(2) To substantiate any positive healthcare effect claimed in accordance with § 9 para. 1, the manufacturer may submit prospective comparative studies as an alternative to the studies under paragraph 1.

(3) Irrespective of whether methods of clinical research or other scientific fields, including but not limited to care or social research, are applied as part of the studies under paragraphs 1 and 2, quantitative comparative studies must be submitted. The selected methodological approach must be commensurate with the positive healthcare effect to be substantiated.

(4) Non-use pursuant to paragraph 1 sentence 1 may consist of non-treatment or treatment without a digital health application. The selected comparator must reflect the reality of care. In deviation from sentence 1, non-use may also consist of treatment with a comparable digital health application. Such other digital health application pursuant to sentence 3 must be finally listed in the directory of digital health applications pursuant to Section 139e (2) and (3) SGB V at the time of the application.

(5) Proof pursuant to paragraphs 1 and 2 must be furnished with the help of studies conducted in Germany. Insofar as studies were conducted in countries outside of the area of application of SGB V, be it in whole or in part, the manufacturer must show that their findings apply equally in a German care context.

(6) The manufacturer must enter studies pursuant to paragraphs 1 and 2 into a public study registry and publish them in full, along with findings, within twelve months of study completion, to the extent that such publication is not opposed by legal requirements pertaining to the protection of business or trade secrets or the protection of personal data or intellectual property. The study registry pursuant to sentence 1 must be a primary registry or a partner registry of the World Health Organisation International Clinical Trials Registry Platform or a data provider of the World Health Organisation International Clinical Trials Registry Platform.

(7) The study reports to be generated as part of the completion of studies under paragraphs 1 and 2 must be prepared in compliance with applicable, internationally recognized presentation and reporting standards.

§ 11

Studies substantiating positive healthcare effects in special cases

(1) In deviation from § 10 para. 1, the manufacturer submits a prospective comparative study to substantiate any positive healthcare effects claimed in accordance with § 9 para. 1 if no suitable data is available to facilitate an informative retrospective comparison and, in particular, no sufficient comparability of populations can be achieved.

(2) § 10 paras. 3-7 applies *mutatis mutandis*.

§ 12

Proof for diagnostic instruments

(1) In the event that a digital health application contains a diagnostic instrument, the manufacturer must determine, by means of a study and in addition to any proof pursuant to § 10, the sensitivity and specificity of the digital health application with regard to the patient group indicated pursuant to § 9 para. 1 number 2 and para. 3.

(2) § 10 paras. 3-7 applies *mutatis mutandis*.

§ 13

Assessment decision regarding adequacy of furnished proof

(1) As part of an assessment decision, the Federal Institute for Drugs and Medical Devices weighs whether the documentation provided sufficiently substantiates positive healthcare effects. The assessment decision considers expected positive as well as negative effects on the basis of available findings, taking into account any special characteristic of the indication, the risk of the digital health application as well as available or unavailable care alternatives.

(2) In the event that the requirements of §§ 10-12 prove unsuitable as proof of positive healthcare effects due to the special characteristics of a given digital health application, the Federal Institute for Drugs and Medical Devices may deviate from the requirements of §§ 10-12.

§ 14

Explanation for improved care delivery

With any application pursuant to Section 139e (4) SGB V, the manufacturer must submit, at a minimum, the results of a systematic data analysis on the use of the digital health application in order to provide a plausible explanation why a trial can produce evidence of positive healthcare effects.

§ 15

Scientific evaluation concept

As part of an application pursuant to Section 139e (4) SGB V, the manufacturer presents an evaluation concept prepared in keeping with generally recognized scientific standards, which takes into account the results of the data analysis pursuant to § 14. The approach explained in the evaluation concept must be capable of furnishing the proof pursuant to §§ 10-12.

Section 4

Supplemental regulations for administrative procedure

§ 16

General provisions

(1) The Federal Institute for Drugs and Medical Devices confirms its receipt of the complete application documents to the applicant within 14 days. Once an application has been received, it may be amended or changed only upon the request of the Federal Institute for Drugs and Medical Devices.

(2) In the event that the manufacturer submits incomplete application documents, the Federal Institute for Drugs and Medical Devices will call on it to complete the application within a period of two to three months, listing all missing documents and information. In the event that no complete application documents are received by such deadline, the Federal Institute for Drugs and Medical Devices must deny the application by issuing a notice to that effect.

§ 17

Procedure for listing for trial purposes

(1) In the event that a manufacturer has filed an application for the entry of a digital health application pursuant to Section 139e (4) SGB V into the directory of digital health applications, and the plausible explanation pursuant to § 14 and the evaluation concept pursuant to § 15 to be submitted alongside the application are adequate for provisional listing, the Federal Institute for Drugs and Medical Devices makes a decision and provides notice accordingly following its receipt of the complete application documents. Such notice will contain information on the duration of the listing for trial purposes as well as on the evidence to be produced pursuant to Section 139e (4) sentence 3 SGB V no later than upon the expiry of the trial period, including any medical services required for the trial.

(2) For final listing in the directory of digital health applications, the proof specified in the notice pursuant to paragraph 1 is to be presented to the Federal Institute for Drugs and Medical Devices in full by electronic means no later than upon the expiry of the trial period.

(3) Just once, the manufacturer may request an extension of the trial period by up to twelve months. For this purpose, the applicant must file an electronic application for an extension of the trial period with the Federal Institute for Drugs and Medical Devices within three months of the expiry of the trial period granted in the notice pursuant to paragraph 1. In the application pursuant to sentence 1, the manufacturer explains the need for an extension of the trial period. Specifically, the manufacturer must argue why the requisite proof cannot be presented by the original deadline and to what extent definitive evidence may be produced if the trial period is extended as requested.

(4) In the event that no application for an extension of the trial period pursuant to paragraph 3 is filed at least three months before the trial period expires, if such filing is incomplete or the application's substance fails to meet the requirements of §§ 10-12, the Federal Institute for Drugs and Medical Devices will deny the application for an extension of the trial period and deletes the digital health application from the directory of digital health applications once the trial period has expired. The manufacturer is to be notified of the deletion pursuant to sentence 1.

§ 18
Significant changes

(1) Significant changes within the meaning of this ordinance are those that

1. amend statements and information published in the directory of digital health applications; or
2. have a significant influence on the fulfilment of the requirements as to

a) the safety, functionality and quality of the medical device;

b) data protection and security; or

c) any proof to be supplied to substantiate positive healthcare effects, including changes to the patient groups for which positive healthcare effects have been or are to be demonstrated for a digital health application.

(2) The Federal Institute for Drugs and Medical Devices will, by electronic means, provide manufacturers of digital health applications with a checklist to help them determine whether a given change of the digital health application amounts to a significant change within the meaning of paragraph 1. In such checklist, the Federal Institute for Drugs and Medical Devices advises manufacturers as to the legal consequences of their failure to give notice pursuant to Section 139e (6) sentences 5 and 6 SGB V.

§ 19
Procedure triggered by significant changes

(1) Once notice pursuant to Section 139e (6) sentence 1 SGB V or the application for the deletion of a digital health application from the directory of digital health applications pursuant to Section 139e (6) sentence 7 SGB V has been transmitted to the Federal Institute for Drugs and Medical Devices, it may be amended or changed only upon the request of the Federal Institute for Drugs and Medical Devices under paragraph 2.

(2) As far as it is learned in the course of the evaluation by the Federal Institute for Drugs and Medical Devices that the information contained in the notice is incapable of supporting a decision on the need to amend the directory of digital health applications or on the deletion of the application from the directory of digital health applications, the Federal Institute for Drugs and Medical Devices may once call on the manufacturer to complete the information within a period of up to three months.

Section 5

Contents and publication of directory of digital health applications pursuant to Section 139 e (1) SGB V

§ 20
Contents of electronic directory

(1) In the directory of digital health applications, the Federal Institute for Drugs and Medical Devices lists the digital health applications that are reimbursable pursuant to Section 33a (1) SGB V. Each digital health application contains a unique directory number. Only the indications specified by the manufacturer may be listed in the directory of digital health applications.

(2) The directory of digital health applications contains the manufacturer information pursuant to § 2 para. 1 sentence 2.

(3) Aside from the information pursuant to paragraph 2, the following data is published, among other information:

1. positive healthcare effects that have been or are to be substantiated;
2. the studies submitted pursuant to §§ 10 and 11 in the form of summaries covering research design and results, including a reference to the place of registration as well as any webpage on which the full studies are published online pursuant to § 10 para. 6;
3. the sensitivity and specificity of the diagnostic instruments contained in the digital health application in accordance with the results of the diagnostic test quality study submitted pursuant to § 12, if applicable;
4. the remuneration sums pursuant to Section 134 (1) SGB V;
5. any additional costs pursuant to Section 33a (1) sentence 4 SGB V, if applicable; and
6. any necessary medical services pursuant to Section 139e (3) sentence 2 SGB V, if applicable.

§ 21
Other features of electronic directory

(1) Additional information from the documents submitted will be published in the directory of digital health applications to the extent that doing so is necessary for purposes of informing healthcare providers, helping patients to make an informed decision about using the digital health application and ensuring that the digital health application may be put to quality-assured use.

(2) The Federal Institute for Drugs and Medical Devices allows information pursuant to § 20 paras. 2 and 3 to be used by third parties as far as doing so is necessary for the use of electronic prescriptions of the services pursuant to Section 33a (1) SGB V. For this purpose, the Federal Institute for Drugs and Medical Devices publishes a suitable interface on

the basis of internationally recognized standards and requests its listing in the directory pursuant to Section 291e SGB V upon the directory's creation.

(3) Starting no later than 1 January 2021, the Federal Institute for Drugs and Medical Devices makes available the information listed in § 20 paras. 2 and 3 in machine-readable and platform-neutral form for processing and publishing purposes to

1. third parties pursuant to Section 303e (1) SGB V;
2. other federal, state or municipal agencies; and
3. charitable legal entities under private law upon request. The Federal Institute for Drugs and Medical Devices establishes the specific terms of data transmission, including but not limited to data formats, of the data use agreement and of users' rights and obligations related to the use of data in user agreements that form the basis of the data use agreement. The user agreements ensure that the data is used without misuse, distorting effects on competition or manipulation. The third party pursuant to sentence 1 must ensure that the origin of the data remains transparent for the insured, the healthcare providers and all other users. This is especially true in the event that the data is used in conjunction with other data. The Federal Institute for Drugs and Medical Devices publishes a suitable interface on the basis of internationally recognized standards and requests its listing in the directory pursuant to Section 291e SGB V.

(4) Starting no later than 1 January 2021, the Federal Institute for Drugs and Medical Devices publishes the information contained in the directory of digital health applications pursuant to § 20 paras. 2 and 3 on a Web portal, using a structure, form and presentation designed to be intuitively accessible to patients as well as healthcare providers.

(5) Starting no later than 1 January 2022, the Federal Institute for Drugs and Medical Devices publishes the information pursuant to § 20 paras. 2 and 3 contained in the directory of digital health applications pursuant to Section 139e SGB V on a barrier-free Web portal, using a structure, form and presentation designed to be intuitively accessible to patients as well as healthcare providers.

(6) With its application, the manufacturer of the digital health application clears the information listed under § 20 paras. 2 and 3 for publication and free third-party use under a license to be determined by the Federal Institute for Drugs and Medical Devices. This applies to the extent that such publication and/or use is not J by legal requirements pertaining to the protection of business or trade secrets or the protection of personal data or intellectual property, and provided further that the manufacturer labeled the information in question accordingly in the application documents and has expressly objected to publication on such grounds.

§ 22

Publication of directory of digital health applications in Federal Gazette

(1) The Federal Institute for Drugs and Medical Devices will place announcements in the Federal Gazette (*Bundesanzeiger*) pursuant to Section 139e (1) sentence 3 SGB V to mark:

1. the creation of the directory of digital health applications;
2. the introduction of new categories or changes to existing categories of digital health applications in the directory of digital health applications;
3. the listing of new digital health applications in the directory of digital health applications;
4. any change to the directory of digital health applications pursuant to Section 139e (6) sentence 1 SGB V; and
5. the deletion of digital health applications from the directory of digital health applications.

(2) The Federal Institute for Drugs and Medical Devices is to see to announcements pursuant to paragraph 1 in quarterly intervals.

(3) In its announcements in the Federal Gazette, the Federal Institute for Drugs and Medical Devices notes the publication of the full wording of announcements pursuant to paragraph 1 in the electronic directory of digital health applications on the webpages of the Federal Institute for Drugs and Medical Devices.

Section 6

Guidance provided by Federal Institute for Drugs and Medical devices

§ 23

Consultation

(1) Upon request, the Federal Institute for Drugs and Medical Devices will provide guidance to manufacturers of digital health applications prior to the submission of an application for the listing of a digital health application in the directory of digital health applications, especially with respect to procedural questions as well as the information and proof to be submitted with the application.

(2) The Federal Institute for Drugs and Medical Devices further advises manufacturers of digital health applications on

1. the obligation to submit proof to substantiate positive healthcare effects, such obligation being imposed on manufacturers under a notice by the Federal Institute for Drugs and Medical Devices pursuant to Section 139e (4) sentence 3 SGB V; and
2. notices of significant changes.

(3) A request pursuant to paragraph 1 is to be filed with the Federal Institute for Drugs and Medical Devices by electronic means. Requests are to be accompanied by documents and proof, such documents and information as the manufacturer may have in its possession at the time, which are of significance to the preparation of an application for the listing of a digital health application in the directory of digital health applications.

(4) The information transmitted to the Federal Institute for Drugs and Medical Devices for the purpose of receiving its guidance pursuant to the foregoing paragraphs is to be held in confidence.

Section 7

Fees and expenses

§ 24
Principles

Subject to the provisions below, the Federal Institute for Drugs and Medical Devices assesses fees and expenses for public services that may be attributed individually.

§ 25
Fees for decisions on listing digital health applications in directory

(1) The fee for the decision pursuant to

1. Section 139e (3) sentence 1 on a manufacturer's application pursuant to Section 139e (2) SGB V; or
2. Section 139e (4) sentences 1 and 3 SGB V

equals no less than EUR 3,000 and no more than EUR 9,900.

(2) The fee for the decision pursuant to Section 139e (4) sentence 6 SGB V equals no less than EUR 1,500 and no more than EUR 6,600.

(3) The fee for the decision pursuant to Section 139e (4) sentence 7 SGB V equals no less than EUR 1,500 and no more than EUR 4,900.

§ 26
Fees for notices of change and deletions

(1) The fee for processing a notice pursuant to Section 139e (6) sentence 1 number 1 SGB V equals no less than EUR 1,500 and no more than EUR 4,900.

(2) The fee for processing a notice pursuant to Section 139e (6) sentence 1 number 2 SGB V equals no less than EUR 300 and no more than EUR 1,000.

(3) The fee for deleting a digital health application pursuant to Section 139e (6) sentences 6 and 7 SGB V equals EUR 200.

§ 27
Fee for consultation

(1) The fee for a consultation for manufacturers of digital health applications pursuant to Section 139e (8) sentence 2 SGB V equals no less than EUR 250 and no more than EUR 5,000.

(2) Advice provided orally, in writing or electronically that is minor in scope is exempted from such fee.

§ 28
Fees in special cases

(1) In the event that an application is denied either in whole or in part, a fee is to be assessed in the amount indicated for the individually attributable public service requested. No fee is assessed if the application is denied solely for lack of jurisdiction of the Federal Institute for Drugs and Medical Devices.

(2) For any decision on an objection, a fee is to be assessed in an amount proportionate to the degree to which the objection fell short of success, such fee not to exceed the amount indicated for the challenged service. In cases of objections aimed solely at the assessment of fees and expenses, the fee equals up to 25% of the amount with respect to which the objection was not upheld. If the objection is unsuccessful for the sole reason that breaches of procedural or formal requirements under Section 41 Social Code Book X are of no consequence, no fee is assessed.

(3) In cases of the withdrawal or revocation of an administrative act, a fee is to be assessed in an amount not to exceed the fee indicated for the enactment of the administrative act in question at the time of withdrawal or revocation, to the extent that such withdrawal or revocation is attributable to the addressee.

(4) In the event that an application is withdrawn or no longer warrants consideration for other reasons before the individually attributable public service has been fully discharged, a fee is to be assessed in an amount of up to 75 percent of the fee indicated for such service. If an objection is withdrawn or no longer warrants consideration for other reasons before it has been formally ruled upon, the fee equals up to 75% of the amount assessed for the challenged service. Unless paragraph 5 provides otherwise, no fee is assessed if the Federal Institute for Drugs and Medical Devices has not yet started processing in earnest.

(5) In the event that an individually attributable public service cannot be rendered by the applicable deadline, or if performance has to be suspended, for reasons attributable to the party in question, a fee is to be assessed in an amount not to exceed the amount indicated for the full service.

§ 29
Other fees

(1) With respect to the following individually attributable public services rendered upon request, fees are to be assessed as follows:

1. for complex written responses in an amount of no less than EUR 50 and no more than EUR 500;
2. for the generation and provision of documents or the generation and provision of electronically stored files, including the conversion of written documents into electronic data, in an amount of no less than EUR 10 and no more than EUR 100, unless this is done as part of individually attributable services pursuant to §§ 25-27; or

3. for file access – unless an objection procedure is pending – in an amount of no less than EUR 25 and no more than EUR 250.

(2) The applicant is to be made aware of the fees associated with individually attributable public services pursuant to paragraph 1.

§ 30

Fee reduction and waiver upon request

(1) At the request of the liable party, the fees to be assessed pursuant to §§ 25-27 may be reduced all the way to 25 percent of the indicated amount if

1. the applicant cannot expect an economic benefit commensurate with such fees;
2. the number of applications is small; or
3. the target audience for which the digital health application is intended is too small.

(2) The assessment of fees may be waived altogether if the economic benefit to be expected is especially small in relation to the amount of fees.

§ 31

Expenses

Section 12 (1) of the Federal Fees Act (*Bundesgebührengesetz - BGebG*) applies *mutatis mutandis* to the reimbursement of expenses.

§ 32

When liability for fees and expenses is incurred

(1) Liability for fees is incurred upon the completion of the individually attributable public service. If such service entails delivery, formal initiation or an announcement, it is deemed to have been completed at such time.

(2) In deviation from paragraph 1, liability for fees in cases in which

1. an application is withdrawn or no longer warrants consideration for other reasons arises at such time; and
2. an individually attributable public service cannot be rendered by the applicable deadline, or if performance has to be suspended, for reasons attributable to the party in question arises at the time of the deadline set for the completion of the service or its suspension.

(3) Paragraphs 1 and 2 apply *mutatis mutandis* to expenses.

§ 33

Party liable for fees and expenses

(1) Liability for payment of fees lies with the party

1. to which the public service is individually attributable;
2. which has assumed liability for the fees owed by another party by so declaring to or informing the Federal Institute for Drugs and Medical Devices; or
3. which is liable for the fees of another party by force of law.

(2) Several liable parties bear liability as joint and several debtors.

(3) Paragraphs 1 and 2 apply *mutatis mutandis* to expenses.

Section 8

Arbitration

§ 34

Composition of arbitration panel and appointment of panel members

(1) The associations pursuant to Section 134 (3) sentence 1 SGB V inform the administrative office pursuant to § 38 of the appointment of members of the arbitration panel according to Section 134 (3) sentences 2-4 SGB V.

(2) The members of the arbitration panel are deemed to have been named as soon as they have informed the associations involved pursuant to Section 134 (3) sentence 1 SGB V that they are willing to serve on the panel.

(3) The members of the arbitration panel are deemed to have been appointed as soon as the associations pursuant to Section 134 (3) sentence 1 SGB V have informed the Federal Ministry of Health that the panel members have been named.

§ 35

Term

(1) The members of the arbitration panel serve for a term of four years. The term of any member newly appointed during an ongoing term of office ends upon the expiry of such term.

(2) In deviation from paragraph 1, the term of the members of the arbitration panel named by the insurance funds and the manufacturers of digital health applications pursuant to Section 134 (3) sentence 2 SGB V ends upon the effective date of the arbitral award.

§ 36

Dismissal and resignation

(1) At the request of a contractual party, the Federal Ministry of Health may dismiss members of the arbitration panel and their deputies for cause. The associations involved must be heard beforehand.

(2) Whenever members of the arbitration panel resign, they must so inform the associations responsible for appointments or the contractual parties, the chairperson of the arbitration panel as well as the Federal Ministry of Health.

(3) Section 134 (3) sentences 4 and 5 SGB V applies *mutatis mutandis* to the appointment of members of the arbitration panel and their deputies, who are succeeding members who did not finish out their term

§ 37

Attending meetings

The members of the arbitration panel are obligated to attend meetings of the panel. In the event that members of the arbitration panel cannot attend, they must notify their respective deputies. Provided that they were so notified, deputies are likewise obligated to attend meetings of the arbitration panel.

§ 38

Administrative office

The administrative office of the arbitration panel is embedded with the National Association of Statutory Health Insurance Funds (*Spitzenverband Bund der Krankenkassen*). It is bound by the chairperson's directions.

§ 39

Initiating arbitration proceedings and deadlines

(1) In the event that a contract on remuneration sums for digital health applications pursuant to Section 134 (1) SGB V fails to materialize, be it in whole or in part, arbitration proceedings commence as soon as a petition is filed with the arbitration panel by either contractual party seeking to bring about an agreement with respect to the contractual terms. Petitions are to be addressed to the chairperson of the arbitration panel in writing or by electronic means. Petitions must contain the following:

1. a discussion of the relevant facts;
2. a summary of the outcome of previous negotiations; and
3. a list of the terms of the contract on which no agreement was reached.

(2) If a contract that has been terminated pursuant to Section 134 (1) was not replaced by another contract, arbitration proceedings commence upon the day following the termination notice period. The terminating contractual party must notify the arbitration panel in writing or by electronic means and recount the relevant facts.

(3) Paragraph 1 applies accordingly to the provisions of the master agreement pursuant to Section 134 paras. 4 and 5.

(4) The chairperson invites the other members of the arbitration panel in writing or by electronic means at least two weeks in advance. Such invitation is to be accompanied by meeting documents that will be the subject of the panel's deliberations.

§ 40

Duty of disclosure

At the arbitration panel's request, the contractual parties must submit the documents needed for panel's decision.

§ 41

Deliberation and ruling

(1) The arbitration panel has a quorum if at least the chairperson and an impartial member of the arbitration panel, or their deputies, as well as one representative each of the health insurance funds and the manufacturer are in attendance. Abstentions are not permitted.

(2) The arbitration panel takes decisions on the basis of oral hearings. The contractual parties, the Federal Ministry of Health, and the patient organizations pursuant to Section 140f SGB V are to be invited to oral hearings. The arbitration panel may also deliberate in the absence of the invitees. The chairperson prepares a transcript of the substance of such deliberations, which may be done electronically as well.

(3) The arbitration panel deliberates and rules in the absence of the invitees. This shall be without prejudice to Section 134 (3) sentence 10 SGB V.

(4) The arbitration panel's chairperson releases the panel's decision in writing or in electronic form, provides grounds for such decision and serves it on the contractual parties involved.

(5) The arbitration panel's chairperson notifies the Federal Ministry of Health as well as the patient organizations pursuant to Section 140f SGB V without undue delay in writing or by electronic means of

1. the institution of arbitration proceedings pursuant to § 39;
2. the arbitration panel's scheduled hearings; and
3. the arbitration panel's decision.

§ 42

Reimbursement and costs

(1) The arbitration panel's chairperson and the two other impartial members, or their deputies, are reimbursed for travel expenses subject to the provisions governing the reimbursement of federal officials for travel expenses according to Travel Expense Level (*Reisekostenstufe*) C. The National Association of Statutory Health Insurance Funds is liable for satisfying such reimbursement claims. To compensate panel members for other out-of-pocket expenses as well as their time, they are given a flat allowance in an amount determined by the National Association of Statutory Health Insurance Funds in consultation with the associations involved. Its final assessment is subject to the approval of the Federal Ministry of Health.

(2) The members of the arbitration panel and their deputies are entitled to be reimbursed for any out-of-pocket expenses as well as to be compensated for their time in accordance with the principles in effect for employees of the associations making appointments or the contractual parties. The associations and contractual parties bear their own expenses associated with the members that they appointed, or their deputies.

(3) The National Association of Statutory Health Insurance Funds on the one hand and the other associations involved with the arbitration panel on the other bear the material and personnel costs of the administration as well as any expenditures pursuant to paragraph 1 for the chairperson and the two other impartial members, or their deputies, in equal parts.

Section 9

Final provisions

§ 43

Effective date

This ordinance comes into full force and effect on the day following its announcement.

Bonn, […] 2020

The Federal Minister of Health

Annex 1

Checklist pursuant to § 4 para. 6

In the checklist below, the manufacturer declares the requirements under § 4 to have been satisfied. It confirms the fulfillment of the requirements by checking the column "Yes."
All digital health applications must comply with the provisions of data protection law as well as the requirements as to data security – basic requirements. Digital health applications that were found, as part of the required analysis to determine the need for protection, to be in need of an elevated level of protection must further meet the requirements as to data security – additional requirements for digital health applications requiring a very high protection level/additional requirements for digital health applications with a very high need for protection.

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
Data Protection					
1	General Data Protection Regulation as applicable law	The processing of personal data by the digital health application and its manufacturer is subject to Regulation (EU) 2016/679 as well as additional data protection regimes, if applicable.			
2	Consent	Is the freely given, specific and informed consent of the data subject obtained for the purposes of data processing set forth in § 4 para. 2 prior to any processing of personal or personally identifiable data?			No consent is obtained since the purpose of processing is the product of a legal obligation of the manufacturer of the digital health application.
3	Consent	Do data subjects invariably give their consents and issue declarations expressly– i.e., by actively taking an explicit action?			No consent is obtained since the purpose of processing is the product of a legal obligation of the manufacturer of the digital health application.
4	Consent	Are data subjects able to revoke their consents with effect for the future easily, without hindrance, at any time and in a readily understood manner?			No consent is obtained since the purpose of processing is the product of a legal obligation of the manufacturer of the digital health application.
5	Consent	Are data subjects advised of their right and related options to revoke consents before such consents are given?			No consent is obtained since the purpose of processing is the product of a legal obligation of the manufacturer of the digital health application.

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
6	Consent	Was the data subject told in clear, unambiguous and user-friendly terms that are appropriate for the target audience which categories of data are processed for which purposes by the digital health application or the manufacturer of the digital health application before consent was given?			No consent is obtained since the purpose of processing is the product of a legal obligation of the manufacturer of the digital health application.
7	Consent	Is the data subject able, at any time, to access the wording of any consent or declaration given by using the digital health application itself or a source referenced in the digital health application?			No consent is obtained since the purpose of processing is the product of a legal obligation of the manufacturer of the digital health application.
8	Purpose limitation	Does the digital health application process personal data exclusively for the purposes set forth in § 4 para. 2 sentence 1 or in another statutory data-processing capacity pursuant to § 4 para. 2 sentence 3?			
9	Data minimization and appropriateness	Is the personal data processed via the digital health application aligned with the purpose and limited to the degree required for processing?			
10	Data minimization and appropriateness	Has the manufacturer of the digital health application made sure that the purposes served by the digital health application's processing of personal data cannot be achieved equally by other, reasonable means that make more economical use of data?			
11	Data minimization and appropriateness	Is health data stored separately from data needed exclusively for the purpose of billing services?			
12	Data minimization and appropriateness	Does the manufacturer of the digital health application make sure that staff tasked with assignments that are not product-related do not have access to health data?			
13	Data minimization and appropriateness	Insofar as the use of the digital health application is not confined to a private IT system of the user: - Does the data protection impact assessment explicitly reflect corresponding use scenarios?			The use of the digital health application is confined to a private IT system of the user.

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
		- Is the insured person explicitly advised that the use of the digital health application in a potentially insecure environment entails security risks that the manufacturer of the digital health application cannot fully address? - Are measures in place to fully avert even the temporary storage of health data on IT systems not used exclusively by the insured person whenever the digital health application is run on such an IT system? - Are files created and data filed locally on the IT system in use securely deleted at the end of each user session of the digital health application even if the user did not explicitly terminate the user session (e.g., by shutting down the IT system used)?			
14	Integrity and confidentiality	Does the digital health application provide for adequate technical and organizational measures to protect personal data against accidental or inadmissible destruction, deletion, corruption, disclosure or illegitimate forms of processing?			
15	Integrity and confidentiality	Is the data exchange controlled by the digital health application, between the data subject's device and external systems, consistently encrypted according to the state of the art?			No personal data is exchanged between the data subject's device and external systems.
16	Accuracy	Does the digital health application provide for technical and organizational measures to ensure that the personal data processed via the digital health application is factually accurate and up to date?			
17	Accuracy	Does the manufacturer take all appropriate action to ensure that any personal data that is incorrect for purposes of its processing is immediately deleted or corrected?			
18	Need for retention	Is personal data collected via the digital health application stored only as long as it must be retained for purposes of delivering the functionalities promised for the digital health application or such other purposes as may arise? directly from applicable legal obligations?			

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
19	Need for retention	Is the storage of personal data discontinued once the purposes according to § 4 para. 2 sentence 1 numbers 1-4 have been fulfilled?			The manufacturer must account for the purposes and state the maximum duration of storage in a separate statement that further explains why such purposes legitimize the continued storage of personal data.
20	Data portability	Does the manufacturer of the digital health application provide data subjects with mechanisms that allow them to exercise the right of data portability from the digital health application, review any personal data that they, the data subjects, provided to the digital health application about themselves in an appropriate format and migrate such data to another digital health application?			
21	Information to be provided	Is the privacy statement of the digital health application easily found and freely accessed and reviewed on the application's website?			
22	Duties of disclosure	Does the privacy statement of the digital health application contain all relevant information on the manufacturer and its data protection officer, the purpose of the digital health application, the categories of data processed for such purpose, the manufacturer's use of such data, the right to revoke consent as well as the options to exercise the rights of data subjects, and does the manufacturer of the digital health application adequately implement any additional duty to provide information under Arts. 13 and 14 of Regulation (EU) 2016/679?			
23	Duties of disclosure	Is the privacy statement of the digital health application either easily found inside or accessed from the digital health application even after the digital health application was installed?			
24	Duties of disclosure	May data subjects obtain information from the manufacturer of the digital health application about the personal data stored about them to the extent decreed in Art. 15 of Regulation (EU) 2016/679?			

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
25	Duties of disclosure	Does the privacy statement of the digital health application contain a comprehensible deletion protocol fulfilling the requirements under Arts. 16 and 17 of Regulation (EU) 2016/679 to address the procedure followed whenever a data subject's consent is revoked and the digital health application is deinstalled, along with the processing of claims for the deletion of data and any restriction of data processing?			
26	Duties of disclosure	May data subjects demand that the manufacturer of the digital health application correct any incorrect and complete any incomplete personal data related to them?			
27	Duties of disclosure	Is the data subject advised of the possibility of the loss of data as well as the right to data portability pursuant to Art. 20 of Regulation (EU) 2016/679 prior to deletion?			
28	Data protection management	Did the manufacturer of the digital health application implement a process for the periodic review, assessment and evaluation of the effectiveness of technical and organizational measures designed to maximize security in processing, which encompasses any and all systems and processes used in connection with the digital health application?			
29	Data protection management	Did the manufacturer of the digital health application impose a duty of confidentiality on all individuals whose responsibilities require access to personal data?			
30	Data protection impact assessment and risk management	Did the manufacturer of the digital health application perform a data protection impact assessment for the digital health application and integrate the risk analysis that forms part of such assessment with the documented processes of a risk management calling for a continuous reassessment of threats and risks?			

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
31	Data protection impact assessment and risk management	Does the manufacturer of the digital health application make sure that breaches of personal data are reported to the supervisory authority within 72 hours of the manufacturer learning thereof?			
32	Data protection impact assessment and risk management	Does the manufacturer of the digital health application implement the provisions of Art. 34 of Regulation (EU) 2016/679 on the notification of data subjects in cases of data protection incidents?			
33	Burden of proof	Did the manufacturer document the data protection guidelines in place for the enterprise and instruct its staff in how to implement such guidelines?			
34	Burden of proof	Has the manufacturer of the digital health application adopted appropriate measures to ensure that it can be reviewed and determined after the fact whether data has been entered, modified or removed, and by whom?			
35	Burden of proof	Is the manufacturer of the digital health application capable of documenting at any time and for any case in which personal data was processed that the data subject's necessary consent had been obtained, unless the processing was undertaken on another legal basis?			
36	Processing on behalf of controller	Is the sharing of personal data with processors via the digital health application or the manufacturer of the digital health application barred, or is personal data shared only with processors that are sufficiently trustworthy and liable, have adopted adequate mechanisms for the protection of any data so received and are bound to the manufacturer under a contractual commitment that rules out any weakening of the promises made vis-à-vis the insured person?			
37	Sharing data with third parties	Is the sharing of personal data with third parties via the digital health application or the manufacturer of the digital health application barred, unless such data sharing is necessary to realize purposes pursuant to § 4 para. 2 sentence 1 number 1 or ensure compliance with legal provisions and is specifically restricted to such aims?			

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
38	Processing abroad	Is health data as well as personally identifiable inventory and traffic data exclusively processed in Germany, in a member state of the European Union or in such country as may be equivalent thereto according to Section 35 (7) of Social Code Book I or on the basis of an adequacy decision pursuant to Art. 45 of Regulation (EU) 2016/679?			
39	Additional protection goals	Is linking personal data across two or more digital health applications technically impossible or do data subjects have to provide their explicit, informed consent for such linking of data, which is to be obtained separately?			The digital health application does not technically support links to or data exchanges with other digital health applications.
40	Additional protection goals	Are measures in place to ensure that no information of or about the data subject is disclosed to the public or a group of persons that the data subject cannot limit, or that such disclosure requires the data subject to actively take explicit action on the basis of information tailored to the intended audience about the nature of any information disclosed and the possible group of recipients?			The digital health application does not support disclosures of information of or about data subjects to the public or a group of persons that the data subject cannot limit.
Data Security					
Basic requirements governing all digital health applications					
1	Information security and service management	Did the manufacturer of the digital health application implement an information security management system (ISMS) pursuant to ISO 27000 series or BSI Standard 200-2 or a comparable system, and can it produce a recognized certificate or comparable documentation to that effect at the request of the Federal Institute for Drugs and Medical Devices?			The application predates 1 January 2022.

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
2	Information security and service management	Did the manufacturer of the digital health application complete and document a structured analysis to determine the need for protection that extends consideration to the damage scenarios "Violation of laws/regulations/contracts," "Interference with right to informational self-determination," Interference with physical integrity of a person," "Interference with performance of duties" and "Negative internal or external effects," which found a normal, high or very high need for protection for the digital health application pursuant to the definition of BSI Standard 200-2, and can it produce such documentation at the request of the Federal Institute for Drugs and Medical Devices?			
3	Information security and service management	Did the manufacturer of the digital health application implement and document processes for release, change and configuration management in due consideration of the requirements under Regulation (EU) 2017/745, which ensure that expansions and adjustments of the digital health application developed by the manufacturer or at its behest have been adequately tested and explicitly cleared prior to going live?			
4	Preventing loss of data	Did the manufacturer of the digital health application make sure that any communication between the digital health application and other services has been technically restricted to prevent any unwanted data communication from the digital health application that may result in the transmission of personal data?			
5	Preventing loss of data	At a minimum, is each data communication among different system components of the digital health application that is conducted via open networks encrypted using the BSI minimum standard for the use of Transport Layer Security (TLS) pursuant to Section 8 (1) sentence 1 of the BSI Act (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik - BSIG*)?			The digital health application does not trigger any data communication that takes place via open networks.

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
6	Preventing loss of data	Does the digital health application verify the authenticity of any service contacted whenever functionalities of the digital health application that are available online are accessed prior to exchanging personal data with such service?			The digital health application offers no functionality that is accessed online.
7	Preventing loss of data	Did the manufacturer of the digital health application make sure that the digital health application does not write unwanted log or help files?			
8	Preventing loss of data	Did the manufacturer of the digital health application make sure that the digital health application does not send out error messages that potentially disclose confidential information?			
9	Authentication	Do all users of the digital health application have to authenticate themselves using a method commensurate with the need for protection of the data processed by the digital health application before they are given access to data available through the digital health application?			
10	Authentication	Have appropriate measures been adopted to ensure that the data used to authenticate the user of the digital health application is never exchanged via unsecured transport links?			
11	Authentication	Does the digital health application use or provide for a central authentication component, which was implemented using established standard components, which is admissible solely for the initial authentication and the trustworthiness of which may be verified through services of the digital health application?			
12	Authentication	Does the digital health application ensure that a user may change the data used for authentication only if information sufficient for a review of the authenticity of such user is provided?			

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
13	Authentication	If the authentication process entails the use of a password: - Does the digital health application compel all of its users to use secure passwords pursuant to a password guideline that requires a minimum password length and defines limits for the number of attempted password entries? - Are measures in place to prevent the plain-text transmission or storage of passwords at all times? - Do logs record any password change or reset, and is the data subject promptly notified of any password change or reset, provided that suitable contact information is available?			The authentication process does not entail the use of a password.
14	Authentication	If the digital health application stores authentication data on a device or a software component situated thereon: Is the user of the digital health application specifically prompted for approval ("opt-in") and advised of the risk inherent in such function?			The digital health application does not store authentication data on a device or a software component situated thereon.
15	Authentication	If information about the identity or authenticity of the user of the digital health application, or about the authenticity of components of the digital health application, is shared via dedicated sessions among components of the digital health application: - Is all session data protected during both exchange and storage using technical means commensurate with the need for protection of the digital health application, and, if applicable, are session IDs generated randomly, with sufficient entropy and using established processes? - Are all sessions set up in an instance of the digital health application invalidated as soon as the use of the digital health application is discontinued or terminated, and may the user of the digital health application force the explicit invalidation of a session? - Are sessions subject to a maximum validity period, and are inactive sessions automatically invalidated after a certain period of time? - Does a session's invalidation result in the deletion of all session data, and are measures in place to ensure that a session, once invalidated, cannot be reactivated even if certain session data is known?			The digital health application does not use sessions.

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
16	Access control	Does the digital health application make sure that each attempt at accessing protected data and functions undergoes an authorization check ("complete mediation") employing – in cases of access by the manufacturer's operating staff – a dedicated authorization component encompassing all protected data ("reference monitor" or "secure node/application"), which is subject to the prior secure authentication of the person seeking access?			
17	Access control	Are all access privileges initially and by default assigned restrictively, and may access privileges be expanded only through controlled procedures that employ effective review and control mechanisms following the multiple-eyes principle in cases of changes to the access privileges for the operating staff of the manufacturer of the digital health application?			
18	Access control	Insofar as the digital health application provides for various user roles: May each role access functions of the digital health application only through the privileges required for the execution of the functionalities associated with such role?			The digital health application does not provide for different user roles.
19	Access control	Does the manufacturer of the digital health application make sure that access to functions and data of the digital health application by the manufacturer's operating staff is limited to secure networks and access points?			
20	Access control	Do all errors and malfunctions related to access control result in access being denied?			
21	Integrating data and functions	Is the insured person confined to the trusted domain of the digital health application, may only trustworthy external contents reviewed by the manufacturer of the digital health application be used from the digital health application and is the insured person alerted in such a case if and when he or she is about to leave the trusted domain of the digital health application?			

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
22	Integrating data and functions	Insofar as the digital health application allows users to upload files: Is this function as restricted as possible (e.g., excluding active contents), are contents subject to a security check and are measures in place to ensure that files may only be stored using the path provided?			The digital health application does not permit data uploads.
23	Logging	Does the digital health application see to the comprehensive, verifiable and corruption-proof logging of all security-relevant events – i.e., those pertaining to the secure identification, authentication and authorization of persons and organizations?			
24	Logging	Is logging data automatically evaluated in order to detect and/or proactively forestall security-relevant events?			
25	Logging	Is access to logging data secured by suitable means of authorization management and limited to few authorized persons and defined purposes?			
26	Regular and secure updating	Does the manufacturer notify data subjects (e.g., by way of push mechanisms or prior to start-up of the digital health application) if and when a security-relevant update of the digital health application was made available for installation or completed?			
27	Secure deinstallation	Are all data and files generated by the digital health application and stored on IT systems controlled by data subjects, including caches and temporary files, deleted when the digital health application is deinstalled?			The digital health application is a purely Web-based application.
28	Hardening	Insofar as services of the digital health application may be accessed using Web protocols: - Are unneeded methods of any protocol used deactivated for all services that may be accessed via open networks? - Are admissible character encodings limited to the most restrictive degree possible? - Have limits been set for access attempts for all services that may be accessed via open networks? - Are measures in place to ensure that no security-relevant comment or product/ version data is revealed?			The digital health application encompasses no services that may be accessed using Web protocols.

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
		- Are unneeded files deleted on a regular basis? - Are measures in place to ensure that search engines will not capture these services? - Are local absolute paths withheld? - Is access to source codes barred?			
29	Hardening	Insofar as the digital health application processes data provided by the data subject or sources not controlled by the digital health application: - Is such data treated as potentially dangerous and validated and filtered accordingly? - Is such data checked on a trustworthy IT system? - Is the automatic handling of wrong entries avoided whenever possible, and are functionalities implemented to that effect in order to rule out misuse? - Is such data encoded in a way that ensures that defective code is neither interpreted nor executed? Is such data separated from specific queries to data-storing systems (e.g., by way of stored procedures), or are data inquiries explicitly protected against attack vectors favored from such data?			The digital health application does not process data provided by the data subject or sources not controlled by the digital health application.
30	Hardening	Are measures in place to ensure that, in all instances, errors in the digital health application are addressed and result in any initiated function being aborted and, if applicable, rolled back?			
31	Hardening	Are suitable protective mechanisms in place to protect the digital health application against automated access if and to the extent that such access would implement unwanted options for using the digital health application?			
32	Hardening	Are technical measures in place to protect configuration data relevant to the secure operation of the digital health application against loss and corruption?			The digital health application does not use configuration data, or such data is not relevant to the secure operation of the digital health application.

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
33	Use of sensors and external devices	Insofar as the digital health application accesses sensors on a mobile device and/or external hardware (e.g., sensors in close proximity to the body) directly: - Did the manufacturer of the digital health application set the framework conditions under which sensors or connected devices may be installed, activated, configured and used, and have such framework condition been put in place to the extent possible before functionalities of this nature are executed? - Does the digital health application ensure that sensors and connected devices were reset in keeping with a documented security guideline when they were installed or first activated for the digital health application? - Can the insured person reset sensors and devices directly controlled by the digital health application to correspond with a documented security guideline? Can data be exchanged between the digital health application and directly controlled sensors or devices only after such sensors or devices have been installed and fully configured?			The digital health application accesses neither sensors on a mobile device nor external hardware.
34	Use of sensors and external devices	Insofar as the digital health application exchanges data with external hardware (e.g., sensors in close proximity to the body): - Are the processes for installing, configuring, activating and deactivating such hardware described in language that is appropriate for the target audience and protected against operating errors to the extent possible? - Do the digital health application and external hardware authenticate one another? - Is data exchanged between the digital health application and external hardware transmitted only in encrypted form following an initial handshake? - Are measures in place to ensure that all data stored on external hardware is deleted when the digital health application is deinstalled or its use is discontinued? - Did the manufacturer of the digital health application document how connected hardware may be deactivated securely, to the effect that no data is lost and no sensitive data remains on the device?			The digital health application does not exchange data with external hardware.

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
35	Use of third-party software	Does the manufacturer keep a full list of all libraries and other software products used in the digital health application, which were not developed by the manufacturer of the digital health application itself?			
36	Use of third-party software	Does the manufacturer ensure by means of appropriate market observation processes that such – as-of-yet unknown – risks to data protection, data security and patient safety as may emanate from such libraries or products are detected in a timely manner?			
37	Use of third-party software	Did the manufacturer establish processes that allow appropriate measures – e.g., blocking the app and notifying its users – to be adopted promptly if and when such risks are detected?			
Added requirements for digital health applications with very high need for protection					
1	Encrypting stored data	Is personal data processed on IT systems not personally controlled by the data subject stored on such systems only in encrypted form?			
2	Penetration tests	Did the manufacturer of the digital health application perform a penetration test for the version of the digital health application to be included in the directory pursuant to Section 139e (1) of Social Code Book V, including all backend components, such test taking into account common attack vectors, such as clickjacking or cross-site request forgery?			
3	Penetration tests	Did the manufacturer of the digital health application document the results of completed penetration tests, along with the results of any work done to implement appropriate measures and recommendations, and transpose them to suitable management systems, if applicable?			
4	Authentication	At a minimum, is two-factor authentication required for the initial authentication of all users of the digital health application?			

No.	Topic	Requirement	Yes	No	Admissible grounds for "No"
5	Authentication	Insofar as the digital health application provides for an option to fall back on single-factor authentication: - Is the user of the digital health application alerted to the risks associated with such option, and does such fallback need to be activated via consent confirmed by an explicit action actively taken by the user? - Can the user of the digital health application re-deactivate such fallback option from the digital health application at any time?			The digital health option does not provide for an option to fall back on single-factor authentication.
6	Authentication	Can the digital health application support the authentication of those insured by the Statutory Health Insurance Fund as the users of the digital health application using an electronic health card with contactless interface no later than 31 December 2020?			
7	Authentication	Insofar as the digital health application assigns a user role to healthcare providers: Can the digital health application support the authentication of healthcare providers as the users of the digital health application using an electronic health professional card with contactless interface no later than 31 December 2020?			The digital health application is not designed for use by healthcare providers.
8	Measures to counter DoS and DDoS	Are messages and data transmitted to services of the digital health application that may be accessed via open network (XML, JSON, etc.) checked for defined schemes?			The digital health application does not exchange data with or between services that may be accessed via open networks.
9	Embedded Web servers	Insofar as the components of the digital health application use Web servers (e.g., for administration or configuration): - Is the Web server configured as restrictively as possible? - Have only needed components and functions of the Web server been installed or activated? - To the extent possible, is the Web server operated under a non-privileged account? - Are security-relevant events logged? - Is access only possible after authentication? - Is any communication with the Web server encrypted?			The digital health application does not use a Web server.

Annex 2

Checklist pursuant to §§ 5 and 6

In the checklist below, the manufacturer declares the requirements under §§ 5 and 6 to have been satisfied. It confirms the fulfillment of the requirements by checking the column “Yes” or, if the admissible grounds provided apply, the column “No.”

No.	Provision	Requirement	Yes	No	Admissible grounds for “No”
Interoperability					
Can the insured person export the data processed via the digital health application in an interoperable format from the digital health application?					
1	§ 5 para. 1 and § 6	Yes, the insured person may export data processed via the digital health application in an interoperable format from the digital health application, for such data to be available for further use by the insured person. Such export proceeds according to a specification of contents of the electronic patient file pursuant to Section 291b (1) sentence 7 of Social Code Book V or in a format recommended in the vesta standards directory of gematik (syntax, semantics), to the extent that suitable specifications had already been published for at least one year at the time of the application. If this is not the case, the export conforms to an open international standard or a profile disclosed by the manufacturer via an open international standard or a standard registered in the vesta directory. If an open international standard or a disclosed profile is used via an open international standard or a standard registered in the vesta directory, the manufacturer has requested that the standard or profile be listed in the vesta directory.			
Can the insured person export the data processed via the digital health application in a form suited to purposes of care from the digital health application?					
2	§ 5 para. 1 and § 6	Yes, the insured person can export extracts of the health data processed via the digital health application relevant to his or her care and pertaining in particular to the course of therapy, therapy planning, therapy results as well as data evaluations from the digital health application starting no later than 1 January 2021. The export shall be implemented in a human-readable and printable format taking into consideration the context of care in which the digital health application is typically used as intended.			

No.	Provision	Requirement	Yes	No	Admissible grounds for "No"
Does the digital health application offer standardized interfaces with personal medical devices?					
3	§ 5 para. 1 and § 6	Yes, the digital health application is capable of assessing data from medical devices used or sensors worn by the insured person for the measurement and transmission of vital signs (wearables) and in this regard supports a disclosed and documented profile of the ISO/IEEE 11073 standard or another disclosed and documented interface (syntax, semantic) that either is listed in the vesta directory or for which the manufacturer has requested such listing.			The intended use of the digital health application does not encompass the exchange of data between the digital health application and medical devices used or sensors worn by the insured person for the measurement and transmission of vital signs (wearables).
Have the standards and profiles used to bring about the digital health application's interoperability been published and may they be used free from discrimination?					
4	§ 5 para. 1 and § 6	Yes, the standards and profiles used to bring about the digital health application's interoperability are published or linked on the application's webpage, and third parties may use them on their systems free from discrimination.			
Robustness					
Does the digital health application withstand malfunctions and operating errors?					
1	§ 5 para. 2	Yes, a sudden loss of power does not result in a loss of data.			
2	§ 5 para. 2	Yes, a sudden loss of Internet connectivity does not result in a loss of data.			
3	§ 5 para. 2	Yes, the digital health application checks measurements, entries and other data from external sources for plausibility.			The digital health application is not capable of assessing data from medical devices, sensors or other external sources, nor does it provide for the entry of data.
4	§ 5 para. 2	Yes, the digital health application encompasses functions for testing and/or calibrating attached medical devices and sensors.			The digital health application is not capable of assessing data from medical devices or sensors.
Consumer protection					

No.	Provision	Requirement	Yes	No	Admissible grounds for "No"
Does the user of the digital health application receive all information needed to make a decision as to use prior to entering into any commitment vis-à-vis the manufacturer or a third party?					
1	§ 5 para. 3	Yes, the information provided for the digital health application on the sales platform or the application website includes a comprehensive description of the scope of functionality as well as the intended medical purpose.			
2	§ 5 para. 3	Yes, the information provided for the digital health application on the sales platform or the application website states in unambiguous language which features are available with the download or use of the application and which features can or must be purchased at what price, for example as in-app purchases or function transfers.			
Is the compatibility of the digital health application with systems and devices communicated in a transparent fashion?					
3	§ 5 para. 3	Yes, the manufacturer of the digital health application publishes on the application website a list of compatibility assurances for operating system versions and mobile devices or Web browsers and Web browser versions, along with additional needed or optionally usable devices, and keeps this list up to date on an ongoing basis.			
Does the manufacturer publish the intended medical purpose of the digital health application?					
4	§ 5 para. 3	Yes, the intended medical purpose pursuant to Art. 2 number 12 of Regulation (EU) 2017/745 or Section 3 number 10 of the Medical Devices Act (*Medizinproduktegesetz - MPG*), in the version applicable through 25 May 2020, is published in the imprint of the digital health application.			
Are the terms of use of the digital health applications consumer-friendly?					
5	§ 5 para. 4	Yes, the digital health application is ad-free.			
6	§ 5 para. 3	Yes, the digital health application is free from untransparent offers, such as automatically renewing subscriptions or temporary special deals.			
7	§ 5 para. 3	Yes, the digital health application has in place measures to protect against unintended in-app purchases or offers no in-app purchases.			

No.	Provision	Requirement	Yes	No	Admissible grounds for "No"
8	§ 5 para. 5	Yes, the manufacturer offers free German-language support to help users operate the digital health application, and such service answers user queries within 24 hours.			
User friendliness and accessibility					
Is the digital health application easy and intuitive to use?					
1	§ 5 para. 5	Yes, the usability style guides of the relevant platform for mobile applications are fully implemented, or alternative solutions were implemented that were shown as part of user tests to offer a particularly high level of user friendliness.			The digital health application is not offered via a platform for mobile applications.
2	§ 5 para. 5	Yes, tests with focus groups that are representative of the target audience have confirmed that the digital health application is easy and intuitive to use.			
3	§ 5 para. 5	Yes, the digital health application will start offering operating assistance for people with disabilities, or it will start supporting the operating assistance provided by the platform, no later than 1 January 2021.			
Supporting healthcare providers					
Does the digital health application inform and support physicians and other healthcare providers involved in the application's use?					
1	§ 5 para. 7	Yes, the manufacturer of the digital health application provides information for any involved healthcare providers, which explains the supplemental use of the digital health application by a healthcare provider as well as the underlying roles for healthcare provider and patient in intelligible terms.			No involvement of healthcare providers is intended for the use of the digital health application.
2	§ 5 para. 7	Yes, the manufacturer of the digital health application provides information for any involved healthcare provider, which describes how best to explain to insured persons the way the digital health application is used as part of therapy.			No involvement of healthcare providers is intended for the use of the digital health application.
3	§ 5 para. 7	Yes, the user may transmit data securely to healthcare providers and give them direct access to his or her data.			No involvement of healthcare providers is intended for the use of the digital health application.
Quality of medical contents					

No.	Provision	Requirement	Yes	No	Admissible grounds for "No"
Does the digital health application rely on established medical knowledge and render such knowledge base transparent?					
1	§ 5 para. 8	Yes, the medical contents and processes implemented in the digital health application are based on the generally recognized professional standard.			
2	§ 5 para. 8	Yes, the manufacturer has put in place suitable processes to keep the medical contents and processes implemented in the digital health application up to date.			
3	§ 5 para. 8	Yes, the sources for the medical contents and processes implemented in the digital health application, such as guidelines, textbooks and studies, have been published and are named in the digital health application or on a website accessible via link in the digital health application.			
4	§ 5 para. 8	Yes, the studies completed with the digital health application have been published and are named in the digital health application or on a website accessible via link in the digital health application.			
Is the health information that the digital health application uses to support users suitable?					
5	§ 5 para. 8	Yes, the health information offered in the digital health application is up to date and based on the generally recognized professional standard.			The digital health application does not offer health information.
6	§ 5 para. 8	Yes, the manufacturer has put in place processes with a view to keeping the health information offered in the digital health application up to date.			
7	§ 5 para. 8	Yes, the sources for the health information offered in the digital health application have been published and are named in the digital health application or on a website accessible via link in the digital health application.			The digital health application does not offer health information.
8	§ 5 para. 8	Yes, the health information provided in the digital health application are presented with an eye toward the target audience.			The digital health application does not offer health information.

No.	Provision	Requirement	Yes	No	Admissible grounds for "No"
9	§ 5 para. 8	Yes, the health information is offered when appropriate and in the context of a given use of the digital health application.			The digital health application does not offer health information.
10	§ 5 para. 8	Yes, the digital health application implements didactic processes to deepen and reinforce the health knowledge offered.			The digital health application does not offer health information.
Patient safety					
Does the manufacturer implement appropriate measures to enhance patient safety?					
1	§ 5 para. 9	Yes, the manufacturer stresses already on the sales platform or prior to start-up of the Web application for which users and indications the digital health application should not be used, to the extent that restrictions do apply.			
2	§ 5 para. 9	Yes, users receive context-sensitive advice as to risks and appropriate measures to mitigate or avoid risks.			
3	§ 5 para. 9	Yes, the digital health application stresses the need to consult a physician or another healthcare provider, or how meaningful such a consultation is, in the context of critical measurements or analytical results.			
4	§ 5 para. 9	Yes, the digital health application recommends that the user terminate or change his or her use of the app if and when a defined condition is found.			
5	§ 5 para. 9	Yes, the digital health application defines consistency conditions for all values entered by the user or collected via connected medical devices or sensors or retrieved from other external sources, such conditions being evaluated prior to the use of a value.			

No.	Provision	Requirement	Yes	No	Admissible grounds for "No"
6	§ 5 para. 9	Yes, error messages in the digital health application are designed to promote the user's understanding of where the error originated and how he or she can help avoid it in the future.			