Federal Office
for Information Security

Deutschland
Digital•Sicher•BSI•

eCare - Digitisation in care

A current market analysis and IT security assessment

Change history

Version	*Date*	*Name*	*Description*
1.0	2020-12-10	BSI, SRC, TÜV Süd	First version

Table 1: Change history

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: referat-di24@bsi.bund.de
Internet: https://www.bsi.bund.de

Content

1 Introduction

The increasing digitisation in the health care system not only provides support in the diagnostic areas at doctors and in hospitals, but is increasingly finding its way into the area of care for the elderly and nursing, too.

On its website, the BMG states that "Digital technologies can help us to better solve the challenges almost all health systems in the western world are facing - more and more elderly and chronically ill people need to be treated, expensive medical innovations need to be paid for, structurally weak rural areas need medical care. New forms of better patient care in the home environment can also be realised. "[1] In the context of the German Nursing Personnel Strengthening Act (PpSG), it is assumed that investments in digitisation " [...] if used properly, have a considerable potential for relieving the burden on nursing staff in outpatient and inpatient care for the elderly [...]"[2].

Some of the recent developments, such as "smart pillboxes" or "smart beds" suggest that such products can reduce the workload of staff and ideally enable patients to lead a more self-determined and comfortable life.

However, these basic examples also make it clear that the trend towards digitisation, combined with a high degree of connectivity, means that on the one hand

- sensitive personal information is collected, which must be processed in accordance with data protection laws (keyword: GDPR) and on the other hand
- very high security requirements in particular - and in contrast to data protection - for the integrity and availability of the processed data are demanded. This is of far-reaching importance when decisions regarding therapy are made or even initiated based on IT.

The necessity to implement IT security measures should be taken into account from the beginning with high priority in terms of product development in the medical field. However, the experience gained in the present study and numerous media reports show that this cannot be assumed to be the case.

It can rather be oberserved that the digitisation of an existing product is often realised by adding communication modules, or previously not connected components are connected to apps or network interfaces – digitisation is therefore realised later as an "add-on". Taking into account the high market pressure with the aim of bringing a digitised "modern" product onto the market in the short term, this approach seems understandable. If the devices are medical devices from risk class IIa, they have to pass a conformity assessment procedure and are being assessed regarding compliance with "safety" features. However, a risk assessment based on a previous vulnerability analysis (from an IT perspective) has often not been carried out and the manufacturer may not even be aware that his product might come with undesirable risks and side effects in a connected and digitalised environment.

The present study therefore aims to obtain a realistic assessment of the IT security situation of currently available "smart" and connected eldery and care products and - without prejudging the outcome - to use the results to raise awareness among the population and in particular among manufacturers regarding the consequences of increasing digitisation and connectivity. This should ultimately lead to developing constructive ideas, which are supposed to allow the implementation of the "security" factor in future developments regarding smart eldery and care products. The point of this study is not to publish individual products and their vulnerabilities, but to get a general and long-term feeling for vulnerabilities that may occur due to connectivity.

[1] https://www.bundesgesundheitsministerium.de/e-health-initiative.html#c2851 visited 16.12.2019
[2] https://www.bundesgesundheitsministerium.de/sofortprogramm-pflege.html#c13622 visited 10.02.2020

2 Project order

With the project *eCare – Digitisation in care,* the current state of connected or "smart" elderly care and nursing products available in Germany, their interface types and an assessment of the IT security of these devices shall be shown.

In the first step, a market analysis was carried out for different product categories available in Germany, which could be used in home, outpatient or inpatient care. In advance of the online research, a care facility and a medical supply store were visited to get an overview of the products that are already demanded in the home care sector and are used in the inpatient sector. Additionally, criteria for the topics were defined in a questionnaire and possible questions to the manufacturers about IT security were conceived.

In the next step, the manufacturers selected in the market analysis were contacted to answer questions regarding the integration of security concepts in their products and, for example, questions regarding the type and content of the transmitted data.

A range of devices found through the market analysis were subsequently procured for the following investigations and subjected to an IT security assessment.

This report summarises the results of the project regarding market analysis and IT security assessment.

2.1 Definition of care equipment

Since there is no formal definition of care equipment (contrary to medical products), the project team defined such equipment as care products that can be used in home or inpatient care. This includes, for example, products for measuring individual vital parameters or those that provide assistance or support in everyday situations of senior citizens or people in need of care. In particular, these are devices that are operated by nursing staff and end users, i.e. not exclusively by specially trained hospital staff and doctors. Exclusive wellness products used, for example, in the fitness or leisure sector were not considered, just like clinical medical devices such as infusion pumps.

2.2 Project team

Members of the project team were employees of the Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn, the TÜV Süd Product Service GmbH (TÜV Süd) in Munich and employees of SRC Security Research & Consulting GmbH (SRC) in Bonn.

The BSI is the central, independent and neutral body for IT security issues. As the federal cyber security authority, the BSI shapes information security in digitisation through prevention, detection and reaction. BSI employees were responsible for the project managment of the eCare project.

The market analysis and survey (chap. 3) were conducted by TÜV Süd employees. As a notified body, TÜV Süd is a recognised institution for the conformity assessment procedures of medical devices on the market relevant for eCare.

SRC employees were entrusted with the investigation and evaluation of the IT security of the devices (chap. 4). SRC bundles current expertise on information technology and its security and is, among other things, a Common Criteria evaluation facility recognised by the BSI. Within the scope of security analyses, SRC evaluates concepts as well as hardware and software of components used.

3 Market overview

In order to obtain an overview of the currently available connected care products, various media were used for search and research. Local contacts were contacted on-site.

The aim was to cover a spectrum as broad as possible of the connected care products available on the German market.

3.1 Identification of product categories

It was necessary to preselect individual product categories in order to facilitate product searches, improve the presentation of results, and to distinguish them from wellness or clinical medical devices, such as infusion pumps.

The product categories were selected based on exemplary visits to a care facility and a medical supply store and online research, which identified a broad product spectrum, from smart beds and smart pillboxes to sensors for vital parameters. The two institutions were selected from the list of those contacted, without any guarantee of completeness. It should be noted that only a few organisations reported that connected care products are in use.

3.1.1 Inquiries and visit to a nursing home

Care products that are already used in the everyday life of people in need of care ought to be found by visiting a care facility. Inquiries to different care institutions showed varying results.

Telephone inquiries to care facilities located in Munich (Stiftung Pfennigparade und Münchenstift GmbH) showed in both cases that no connected care products were used. The Pfennigparade foundation is a care facility for people with disabilities. The Münchenstift GmbH is a care facility for senior citizens.

Furthermore, the facility of the HSH Hohenloher Seniorenhilfe GmbH in Öhringen was visited. In this facility, several connected care products are already in use to increase the well-being of the residents, as this makes it possible to avoid other measures, which are explained in more detail below.

Two of the connected products used there are listed below:

- The Dementia Care System is a system for senior citizens who are still able to move well and independently, but could lose their orientation. They are equipped with wristbands, which in combination with other hardware components set off an alarm to the nursing staff when the buildings are left through their exits. The generated alarms contain information about the persons who have left the building and where they have left it.
- Wireless alarm foot mats consist of a mat system and a wireless receiver module, which is connected to the call system of the building. On the one hand, it serves to detect elderly people at risk who should not leave their room alone at night. For this purpose, the mat is placed in front of the senior's room and an alarm is triggered when the mat is stepped on. On the other hand, it is used to detect attempts to stand up by seniors at risk of falling. For this purpose, the mat is placed next to the senior's bed. The alarm is also triggered when stepping on the mat.

3.1.2 Visit to a medical supply store

Medical supply stores offer on-site availability in terms of supply and advice on the provision of aids. Apart from online shops, they are much more often the primary contact for older people.

A medical supply store in Munich was asked about current products and an initial overview could be obtained. The available product catalogues are especially useful for those who do not have access to online shops.

3.1.3 Conclusion

From a first online overview research and the visit to a nursing home and a medical supply store, a set of 14 product categories could be defined. Those are:

1. Home emergency call systems through an actively triggered emergency call from the senior
2. Monitoring of senior citizens through passively triggered alarms, such as unsupervised standing up
3. Camber and obstacle detection
4. Smart beds
5. Physical assistance, such as stairlifts or bathtub lifts
6. Smart glasses and reading aids
7. Smart dishes and pillboxes
8. Sleep monitoring
9. Reminder services with a nursing background
10. Interaction services for movement and social interaction with therapeutic background
11. Connected rollators and wheelchairs
12. Connected heated blankets
13. Connected sleep apnoea therapy devices
14. Connected devices for vital data measurement, such as blood sugar, blood pressure, temperature or blood clotting.

3.2 Available care products by category

Based on the various product categories, the next step was to conduct a detailed online research to find connected care products available in Germany.

3.2.1 Internet research

The internet research was carried out using search engines according to product categories or individual search terms. As a result, online shops of medical supply stores, websites that focus on connected homecare and care products, blogs, individual articles or other news magazines that deal with the topic of "Smart Care", were visited. The research took place over a period of approximately six weeks and was completed on March 15, 2019. New products available on the market after that period were not taken into account.

The following information ought to emerge as a result of the internet research on connected care products:

1. Manufacturers of connected care products and their products – different manufacturers partly offer several connected care products
2. Contact details of the manufacturers: phone number, e-mail address and mailing address
3. Product descriptions - functions of the devices
4. Interface used, e.g. Bluetooth, Wi-Fi
5. Link to the product pages and manufacturers
6. Location of manufacturers
7. Link to the manufacturers‘ online shop, if applicable
8. Price of the products

3.2.2 Conclusion of the Internet research

133 connected care products were identified as a result of the internet research. Devices capable of measuring vital data were found most frequently.

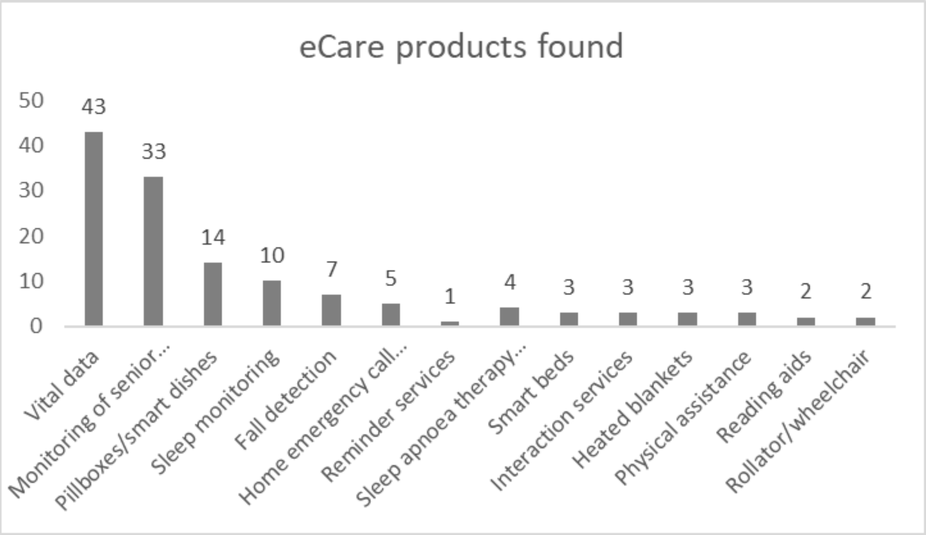


Figure 1: Market research overview for connected products

- Connected devices for measuring vital data

In total, 43 products for measuring vital data from 20 different manufacturers were identified. Those include connected pulse oxymeters, temple thermometers, blood glucose meters, blood pressure meters and body analysis scales. According to the manufacturers, 93% of these are equipped with Bluetooth modules and the remaining with Wi-Fi modules. These products focus on healthcare apps of the respective manufacturers which receive the measured parameters such as weight, heart rate, blood pressure or even the glucose level in the blood measured by the actual measuring devices, store them and evaluate them if necessary. Some manufacturers have a larger product portfolio, so that the user can record and track various parameters from one or more products.

- Monitoring of senior citizens

Second most common, 33 devices in the category of monitoring of senior citizens from 21 different manufacturers were found. These include products for step detection, for detection of getting out of bed and floor sensors for fall monitoring. In addition, protection systems for people suffering from dementia with transponder wristbands, smart watches with GPS positioning function or access control systems were found. For those products, the radio standards were not always specified (36%). This means that in about every third of the 33 smart products for monitoring of senior citizens found, no information on the radio standard used was provided by the manufacturer in the product description.

The vast majority, 39% of the 33 identified products for monitoring of senior citizens, are equipped with a proprietary radio standard. Another 18% have a Wi-Fi function and 6% a Bluetooth function. 9% integrate an RFID component and the remaining 12% of products are equipped with a GSM module. Sometimes several different radio standards are used in one device. The corresponding alarms or localisation data are transmitted either to a house call system or to an app.

- Pillboxes/smart dishes

Of the connected products found, 14 are pillboxes or smart dishes from 13 different manufacturers. 79% of them are equipped with a Bluetooth module. For one product, no information on the radio standard used was provided. Two other products are equipped with a GSM module or Wi-Fi module. The main functions of these smart devices are a reminder for taking pills or for taking liquids directly implemented in the product and a notification for relatives, or storage of the data about the intake in an app. Other functions include measuring and changing the temperature of the cup/bottle contents.

- Sleep monitoring

In total, ten connected devices for sleep monitoring from eight different manufacturers were found. Seven devices are equipped with a Bluetooth module. Two manufacturers integrated a Wi-Fi module. Two other manufacturers do not provide information on the interface used. One manufacturer uses a GSM module in addition to the Wi-Fi module. The implemented device functions of smart sleeping mats or pillows are used to monitor sleep through sensors, to record movements, heart and breathing rate or snoring through a microphone, which are transmitted wirelessly and are recorded in an app.

- Fall detection

Seven of the products found could be assigned to the category fall detection. Of these, a GSM module is installed in six products. One manufacturer uses a GSM module in addition to the Wi-Fi module. One manufacturer does not provide information on the interface used. All devices use GPS data to locate the person, some of which have an integrated additional emergency call function. The data is collected via app and notifications are generated. The devices are designed as a Smartwatch, as a wristband with an integrated sensor or as a keychain.

- Home emergency call systems

Five different devices from five different manufacturers were identified in the product category of home emergency call systems. Three manufacturers claim to use a proprietary radio standard. One device is equipped with a GSM module, another manufacturer only refers to an internet connection in general. These systems are partly based on such type of call systems where GPS localisation information of the sensor the respective person wears is used

- Sleep apnoea therapy devices

In the category of sleep apnoea therapy devices, four products from three different manufacturers were identified. Three of the four devices are connected via a Bluetooth interface. One manufacturer does not provide any specific information. The corresponding app can be used to operate the device and serves to display and record the parameters.

- Smart beds, heated blankets and physical assistance

One device each was identified three times in the group of beds, three each in the warming blankets category and three more in the physical assistance category.

There is no information on the radio standard for the smart beds found. The integrated stand-up detection and weighing are implemented device functions.

The heated blankets are equipped with Wi-Fi and Bluetooth functions or no details are given. The desired temperature of the heated blanket can be controlled remotely via app.

According to the manufacturers, only proprietary radio standards are used in the category of physical assistance. The products found are stairlifts with integrated remote controls.

- Reading aids and rollators

Two products each were found in the category reading aids and rollators. Those, as well as the reading aids, have a GSM module and a Bluetooth module integrated. The reading aids can be controlled via app. The rollators transmit GPS data, make emergency calls or warn when integrated sensors detect obstacles.

- Reminder services

One device found in the reminder services category has been implemented in the form of a tablet with a reminder service for senior citizens, which can be linked to other smartphones via Wi-Fi.

In general, it can be said that connecting hardware components of care products, such as oxygen saturation sensors or thermometers to an app, serves the purpose of wireless data transmission on the one hand and the storage of data in a cloud for a longer period of time on the other hand. This allows the user a certain freedom of movement, as the sensor or thermometer is not wired, as well as an overview of his personal vital parameters over a certain period with a corresponding evaluation. For devices with integrated positioning services, the wireless GPS module, including alarming or sending a message, represents the connected functionality.

In the context of contacting the manufacturers of the products found, it was useful to get an overview of the different locations of the headquarters. The following figure shows that most of the manufacturers have their headquarters in Germany (41). The second most frequent manufacturer locations are the USA (11), followed by Switzerland (4), France (4), the Netherlands (4), Great Britain (3), Italy (2), Belgium (2), Hongkong (2), Sweden (2), Austria (2), Spain (1), China (1), Finland (1), Singapore (1), Slovenia (1), and Turkey (1).

One objective of the project was to identify smart, connected care products, which are actually available in Germany. This selection criterion explains the accumulation of manufacturer locations with 80% in the EU (incl. Switzerland). About 20% of manufacturers are located in non-EU countries.

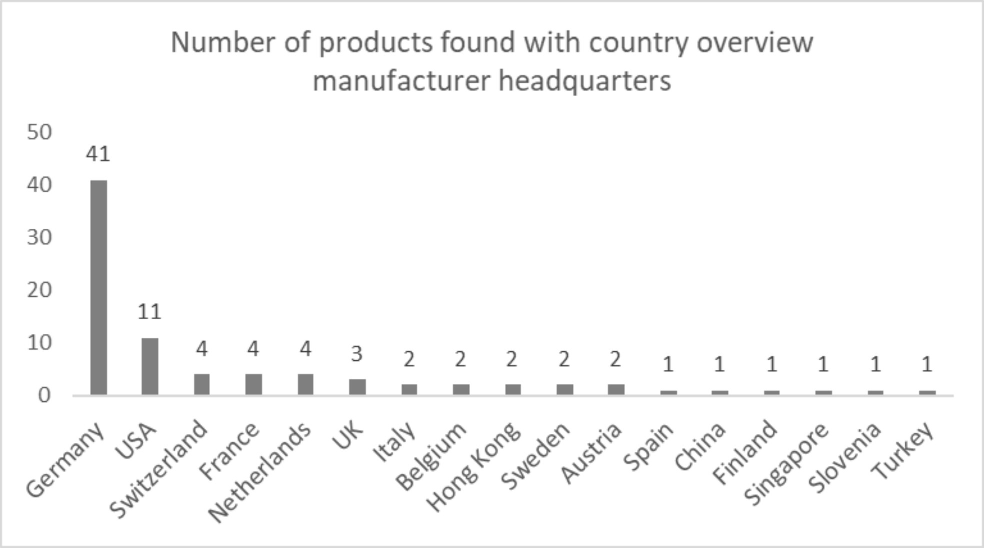


Figure 2: Overview of the main locations of the manufacturers of the identified connected care products

The following overview serves to show the price segment into which products for home and/or outpatient/inpatient care can be put. It is striking that the price range differs widely in some cases, which could be due to, among other things, the different range of functions.

Among the devices for vital data measurement, the most expensive device, which is approved as a medical device is offered for 670 €. On the other hand there is a product that costs about 20 € and is also declared as a medical device.

Among the rollators, a high-priced model was identified. It comes with a variety of functions, such as GPS tracking, automatic brakes and an emergency call function (2890 €). The smart walking stick, which vibrates when obstacles are detected, is much cheaper (399 €).

Product category	**Price range**
Vital data	20-670 €
Monitoring of senior citizens	50-1400 €
Pillboxes/smart dishes	60-318 €
Sleep monitoring	58-300 €
Fall detection	108-199 €
Home emergency call systems	N/A
Reminder services	240 €
Sleep apnoea devices	735-990 €
Smart bed	N/A
Interaction services	789 €
Heated blankets	160-254 €
Physical assistance	N/A
Reading aids	N/A
Rollator/wheelchair	399-2890 €

Table 1: Price overview of connected care devices

3.3 Self-assessment of the manufacturers

The online research did not result in any information on the IT security standards used for connected care products. In the next step, all manufacturers identified so far were contacted in order to encourage them to participate in the developed survey. They were asked to answer questions regarding the implementation of IT security aspects in their connected care products available on the market.

3.3.1 Creation and structure of a catalogue of questions

For the online survey a catalogue of questions was created. The purpose of the questionnaire was to gain a minimum amount of information regarding the IT security integration for the respective product.

To achieve this objective, the following structural requirements ought to be met:

- Designing questions in such a way that different categories are sufficiently considered
- Minimising the scope to obtain a maximum number of responses

As a basis for the creation of the questionnaire, various literature sources were used to narrow down the questions or, for example, to identify certain selection options.

The questionnaire comprises twelve questions on the subject of IT security with mainly yes/no questions and a question about the product range of the manufacturer. In the survey, the manufacturer chooses his product category from a list of the specified product groups. The questions were solely formulated in English.

3.3.2 Procedure for conducting the survey

In order to carry out the survey, it was initially planned to send out the questionnaire as a PDF file. However, ensuring anonymity would not have been plausible and manufacturers would have to invest more/extensive effort in the conventional process of filling in and returning the form.

Consequently, the link to the online question tool was sent to each manufacturer. The online survey was conducted via the survey tool from easyfeedback GmbH. Using this tool, anonymity could be preserved, data could be evaluated and an overview of the number of participants could be received.

The first contact with the manufacturers was made, if possible, by telephone. An interview guide was prepared in the run-up to the interview. The objective was to talk directly to the respective quality management representative. This person was provided with a brief explanation of the matter and asked to confirm his or her willingness to participate in the survey. If consent was given, an e-mail describing the aim of the project and the survey thereby proividing the link for the surveyto the contact person.

If telephone contact was not possible, the manufacturer was contacted via e-mail or via the respective form on his website. Those who had expressed their willingness to participate were reminded by e-mail about two weeks after the first contact. The increasing number of visitors to the online survey could be observed continuously. After the second reminder to participate in the survey was sent, no further contacting was initiated. The collection of answers was completed on May 14, 2019.

In total, 52 out of 84 manufacturers were contacted by telephone thereby introducing the topic IT security of connected care products. 11 contact persons communicated they no longer wish to participate in the survery. 41 out of the 52 contacted manufacturers received a directly addressed invitation to the survery. For those manufacturers who could not be reached directly by telephone, the link was sent via the contact form on their website or the general contact e-mail address to enable participation in case of interest. In total, the survery link was sent to 60 potential participants. Among them 19 participants were not available by telephone but 41 were successfully contacted by telephone prior to the survey.

The number of manufacturers who have not communicated their willingness to participate in the survey and the total number of e-mail invitations for the survey do not represent the total number of manufacturers found in course of the market search. This is due to several reasons. Some manufacturers identified were not the original manufacturers (OEMs) and therefore not capable to answer the questions. In some cases the respective OEM was listed under a different name and had already been contacted. Manufacturers with devices containing only a proprietary radio standard were neither contacted nor included in the survey.

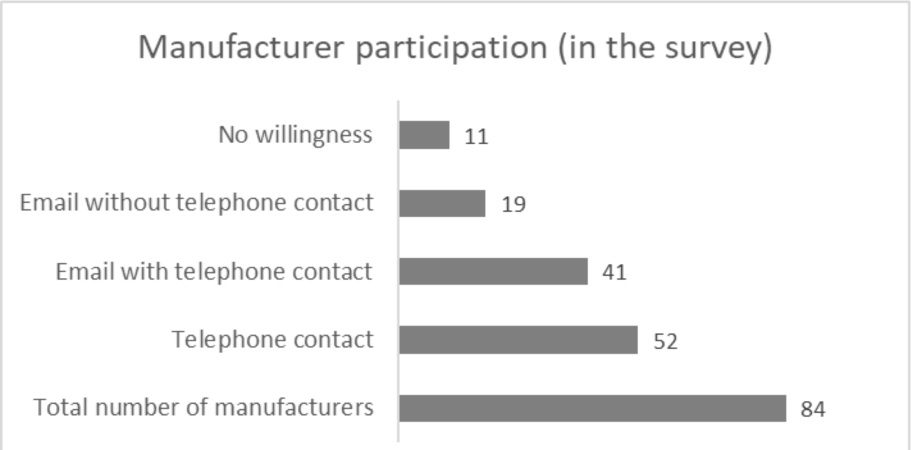


Figure 3: Overview for contacting the manufacturer and signalled willingness to participate

In total, 60 out of 84 manufacturers were invited to participate in the survery, of whom 41 were contacted directly by telephone.

The online survey was accessed 35 times. Twelve participants answered all questions. This results in a participation rate of 20% (twelve out of 60 of the invitations sent were answered completely).

3.3.3 Conclusion and evaluation of the questions

In the following section, individual questions ofconcerning the IT security of the identified connected care products are discussed in more detail. For this, the intention of each question, the participants' results as well as an answer-based interpretation are listed.

1. **Please select the type of your connected care product!**

   The question refers to the category of the connected care product. As described in chapter 3.1.3, only the product categories preselected based on the market researchcould be selected.

   Objective: The online survery was conducted anonymously. Before answering the questions, participants were asked to assign themselves to one of the product categories given. Hereby it was possible to evaluate answers regarding the product category later. This question was a mandatory question and just one category was supposed to be selected.

   Conclusion: Of a total of twelve survey participants, three belong to the category of vital data measurement, two each to the category of monitoring of senior citizens, sleep apnoea therapy devices and smart beds and one participant each to the category of interaction services, reading aids and home emergency call systems.

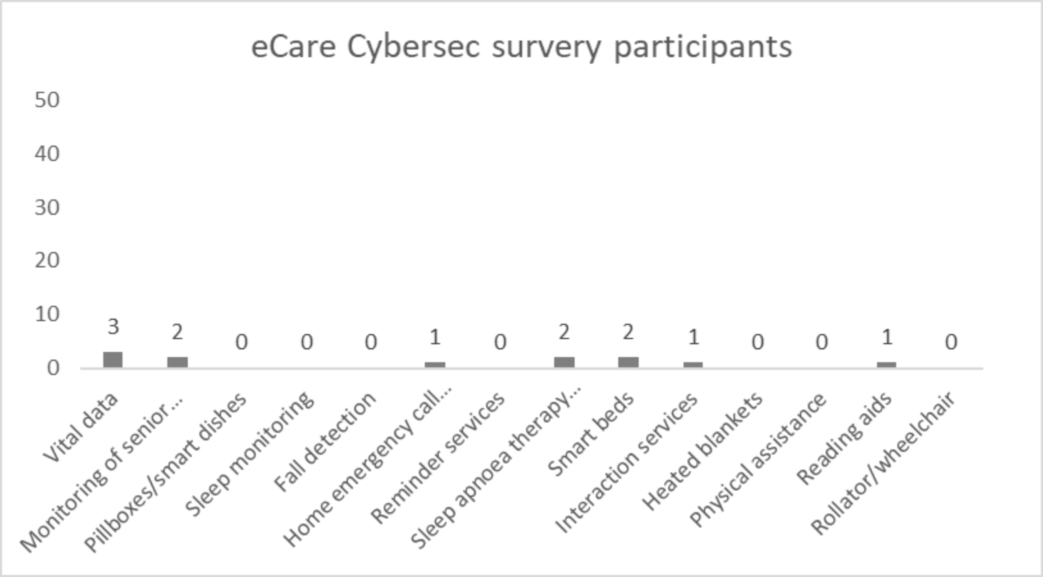


Figure 4: Number of participants by product categories

Interpretation: Considering all product categories, it is striking that there are devices with and without a CE mark (certified medical device). It could be concluded, that those manufacturers who are already aware of cyber security issues due to regulatory requirements in the area of medical devices, are likely to consider such standards and exhibited a higher willingness to participate in such a survey, in contrast to those manufacturers who are, for example, active in the consumer sector. Furthermore, there was no obligation for manufacturers to participate. Surveys are perceived as time-consuming and do not benefit the respondents themselves. In the categories of sleep apnoea therapy and vital data measurment, such CE-marked medical devices were available within the scope of the product selection. Product categories from which no participation in the survey could be identified were, for example, pillboxes or sleep monitoring. The majority of these manufacturers is not located in Germany.

2. **In what kind of network environment is your device meant to be operating?**

   Objective: The thematic question relates to the types of networks used. The options were: Wireless point-to-point (e.g. Bluetooth connection), intranet (wired, wireless), internet (wired, wireless incl. mobile connections) or others (with request for specification). The participant was asked to choose at least one option. The question ultimately aims at different requirements resulting from the use of a Bluetooth connection or the use of wireless or wired intranet or internet connections.

   Conclusion: Five of the twelve participants state that they use a wireless connection, such as Bluetooth. More specifically, this is used in the category of sleep apnoea therapy devices once, twice in the category of smart beds and twice in the category of vital data measurment. Intranet use (wireless or wired) is stated three times in total, once each in the categories of vital data measurment, glasses/reading aids and smart beds. The use of internet connections is stated four times, once each in the category of monitoring of senior citizens, in the category of emergency call systems, in the category of sleep apnoea therapy devices and in the category of vital data measurment devices.

   The use of other standards was stated a total of three times, specifically a low voltage bus system for monitoring of senior citizens and a hard-wired one, according to DIN VDE 0834, for one interaction service and another without concrete specification.

Interpretation: Five specified Bluetooth connections face seven intranet/internet connections. For a Bluetooth connection to be established, maintained and for communication to take place, a certain maximum distance must not be exceeded. In contrast, access via intranet and internet is not limited to a physical distance.

3. **Was cyber security part of your device design/development from the beginning?**

   Objective: The purpose of this question was to determine the extent to which the participants had taken the issue of cyber security into account during device development. Only the answers "yes", "no" or "not sure" were selectable. In the case of "no" or "not sure", the participants were asked to continue with the next but one question.

   Conclusion: Three of twelve participants state that it was not the case. Nine of them confirmed the question. The participants, who did not consider cyber security from the beginning, belong to the product category of interaction services, reading aids and monitoring of senior citizens.

   Interpretation: Here, it can be determined as well that the total number of participants is a result of the fact that they are already familiar with the topic and also knew how to put all questions into the right context. In addition, it is evident that even those who claim not to have considered cyber security from the beginning, integrated certain security concepts later. The remaining potential participants, who had visited the survey site but did not participate, might have not been able to answer the questions in a dedicated way and therefore may not have had any connection to the topic of IT security.

4. **Which of the following options were part of your cyber security device design/development?**

   Objective: The question was intended to point out certain security measures, i.e. even those participants, who were not familiar with the topic, were able to get an overview. At least one option had to be selected. The options were: security concepts, development policies, security gates, code analysis, own penetration tests, 3rd party tests (incl. 3rd party penetration tests, certification by third parties or others with the request for specification). The individual measures offer different advantages and disadvantages with different levels of security.

   Conclusion: Nine participants state that they use a security concept. Six of them state that a specific development policy is used. Four participants each use code analysis and tests carried out by third parties including penetration tests. Own penetration tests are indicated three times. Two participants state that they are certified by third parties and one participant states other measures are in place but without specifying them further.

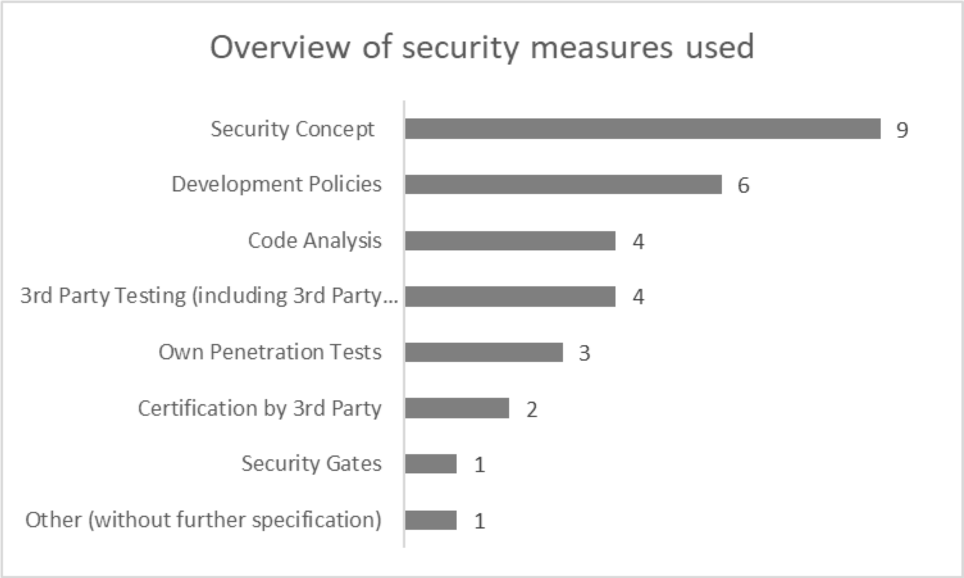


Figure 5: General overview of the specified IT security measures

It means that on average 2.5 different security measures are stated per participant. In detail, it can be observed that some manufacturers are familiar with security measures and implement a variety of them, e.g. a manufacturer of a device for monitoring of senior citizens and a manufacturer of a reading aid. They state that four different security measures are implemented. One participant from the product category of vital data measurement states that five different security measures are deployed. When comparing the answers of the two participants, who belong to the same product category of monitoring of senior citizens, a broad spectrum of implemented measures can be observed. On the one hand, four different security measures are mentioned and on the other hand none are. This participant also stated, that cyber security was not considered from the beginning (see question 3).

Within the category of sleep apnoea therapy devices it can be revealed that three different security measures are used in each case. Both manufacturers used different measures.

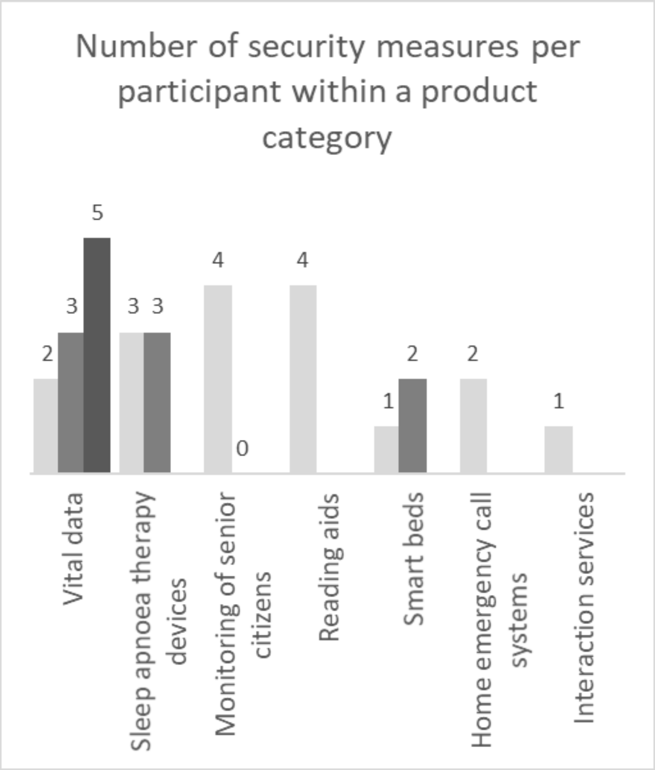


Figure 6: Overview of IT security measures used according to product categories

Interpretation: Of the twelve participants, the use of IT security measures is quite different, ranging from the use of a large number to none. No focus on specific measures can be identified within a product category either. No conclusion can be drawn that the number of security measures used correlates with the criticality and number of functions.

5. **Does your device have a role system with different privileges?**

Objective: The objective was to determine the extent to which various user data, treatment parameters, and basic settings could be changed. Different logins were to be logged and passwords were to be stored cryptographically rather than as plain text.

Conclusion: Seven of twelve participants answer the question with "yes". Four participants state that their system does not come with a role system allowing for different privileges. Of these, two participants belong to the product category of vital data measurement, one participant to the category of sleep apnoea therapy devices and one participant to the category of interaction services. One participant is not sure whether the question applies to his system. This participant belongs to the product category "smart bed".

Interpretation: This means that about 60% of the participants have realised the importance of different authorisation levels. It can be concluded that they have implemented different login rights, i.e. different users have different permissions and access to modify sensitive data is restricted. It is not clear if physical separation is guaranteed by this, since access via the service mode, for example, may possibly allow to change treatment parameters.

6. **Does the interface offer a remote control of the device?**

   Objective: The question refers to the protection of the device during online access. Any remote access control should offer account restrictions and monitoring of logins, including failed login attempt.

   Conclusion: Eight out of twelve participants state that it is possible to access the device remotely. Three participants answer with "no". It is noteworthy at this point that all three participants belong to the product category of vital data measurement. One participant is not sure.

   Interpretation: Any online remote access allows additional external access and represents a potential security risk if it is not appropriately secured. Remote access to the device is possible for almost each of the selected product categories, except for vital data measurement devices. It is unclear to which extent the term remote is understood and interpreted by the respective participant, i.e. whether remote means exclusively "remote access" or also "wireless remote control", e.g. in the same room.

7. **Does the transferred data include patient data (e.g. name, age)?**

   Objective: The next question addresses data security and possible types of data, which could be transferred. Only one answer could be chosen: "yes", "no" or "not sure".

   Conclusion: Three of twelve participants state that they transfer patient data, such as age and name. Of these, two participants belong to the vital data measurement category and one participant to the sleep apnoea therapy devices category. Nine participants chose the answer "”no".

   Interpretation: Since the handling of sensitive data is seen as a critical issue, 75% of respondents say that they do not transfer any. However, this does not mean that the products do not collect patient data.

8. **Is all communication encrypted using a secure kind of protocol? (e.g. https instead of http, ssh instead of telnet, sftp instead of ftp)?**

   Objective: The participant is asked whether the product uses possible standards for internet communication.

   Conclusion: Ten out of twelve participants confirm that they use a secure, encrypted connection such as https, ssh or sftp. This means that ten of twelve participants use an internet or intranet connection.

   Interpretation: However, when comparing this result with the result of question 2, where in total seven of twelve participants state that they use an intranet or internet connection, this seems contradictory. The participants seem to consider encrypted communication appropriate.

9. **Is all stored data encrypted with a state-of-the-art method?**

   Objective: The objective was to find out if the data, in particular sensitive personal data, is encrypted and thus securely stored.

   Conclusion: Two participants state that not the entire data is encrypted with state of the art methods. Those participants belong to the vital data measurement category. The third participant of said category does not make a statement on this. One participant of the smart bed category is not sure. Eight participants are sure. They use state-of-the-art methods to encrypt all data.

Interpretation: Considering the two participants producing vital data measurement devices but do not encrypt all data with state-of–the-art methods it becomes clear, that those are the same participants stating to transfer patient data, such as age and name.

10. **Is it ensured, that an impaired communication interface (e.g. too many requests, unexpected moment and/or type of request) does not disturb the basic functionality of the device?**

    Objective: The objective of the question is the unrestricted assurance of basic device functions, which should operate independently from the communication interface. For example, have interruptions in the connection etc. been taken into account or have simultaneous multiple accesses been simulated?

    Conclusion: Nine of twelve participants state that e.g. too many requests do not disturb the device function. Three participants cannot confirm this. Those participants who do not confirm this belong to the product category of smart bed, monitoring of senior citizens and vital data monitoring.

    Interpretation: Apparently, this part of a possible security vulnerability is recognised by 75% of the participants and appropriate measures are taken.

11. **Is there a regular update/patching cycle/process for your device?**

    Objective: The purpose of this question is to determine the extent to which recurring updates, e.g. for debugging, adaptation of new standards, etc., are already planned during the development process.

    Conclusion: Three participants state that this is not intended for their devices. Nine participants confirm to offer an update or patch function.

    Interpretation: With the percentage of participants who perform updates and patches on their devices, it becomes possible to fix vulnerabilities, both in the programme code and in relation to newly identified potential security vulnerabilities.

12. **Are updates/patches checked on their authenticity?**

    Objective: The objective was to determine the extent to which checkpoints are set for updates/patches before the update/patch is executed and how to prevent malicious programmes from interfering with or influencing the main functions of the device.

    Conclusion: Only one manufacturer does not check updates or patches for authenticity. This manufacturer belongs to the vital data measurement category. Eight participants check updates/patches for authenticity. Two participants are not sure about this. Those participants belong to the sleep apnoea therapy devices and vital data measurement product category.

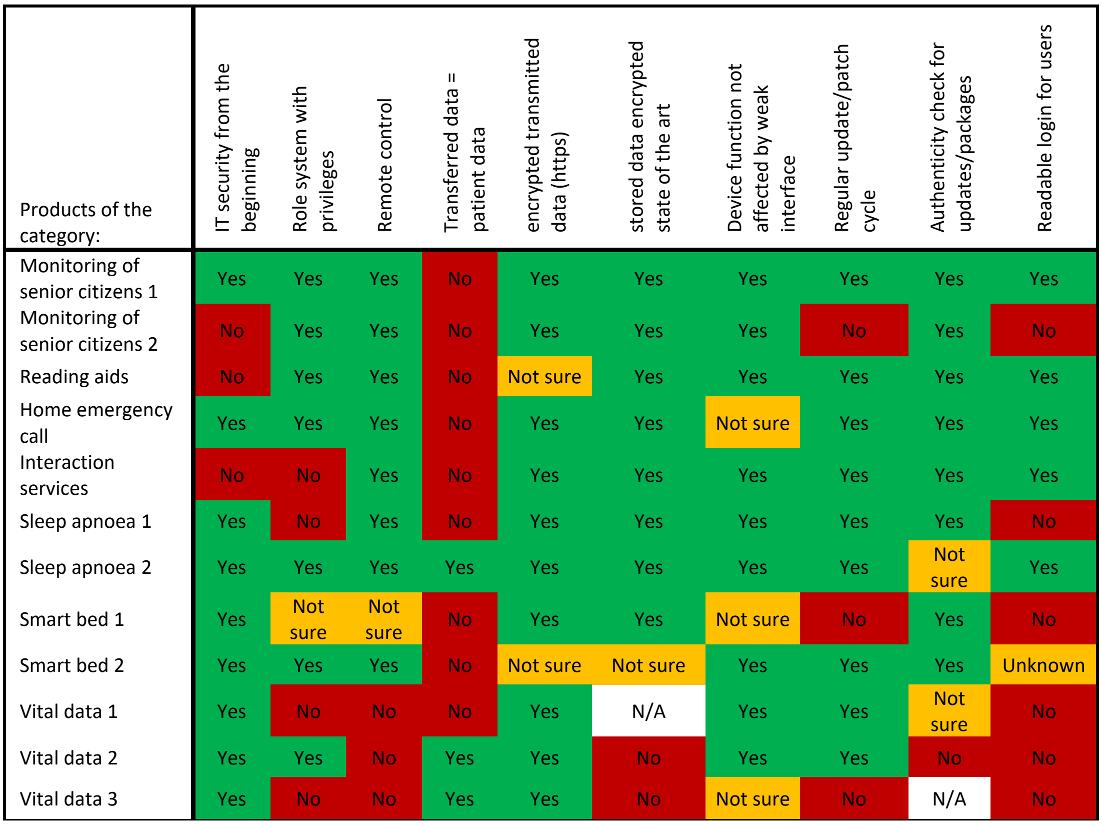
    Interpretation: 90% of participants are aware of the importance of authentication and implemented it in their devices. A small number of participants is not aware of this fact or unable to answer this question.

13. **Does your device provide logging, readable to the user, to detect e.g. intrusion attempts or other possible suspicious activities?**

    Objective: For example, are failed logins logged and made visible to the user, or are users able to detect irregular activity?

Conclusion: Six participants chose "no". Three of them belong to the category vital data measurement. Five participants confirm that intrusion attempts or other conspicuous intrusion attempts are logged. Only one participant is not sure about this. This one belongs to the smart bed category.

Interpretation: Half of the participants seem to be unaware that this is a way to detect potential hazard and to take appropriate action (e.g. changing login data, contacting the manufacturer).



Products of the category:	IT security from the beginning	Role system with privileges	Remote control	Transferred data = patient data	encrypted transmitted data (https)	stored data encrypted state of the art	Device function not affected by weak interface	Regular update/patch cycle	Authenticity check for updates/packages	Readable login for users
Monitoring of senior citizens 1	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Monitoring of senior citizens 2	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No
Reading aids	No	Yes	Yes	No	Not sure	Yes	Yes	Yes	Yes	Yes
Home emergency call	Yes	Yes	Yes	No	Yes	Yes	Not sure	Yes	Yes	Yes
Interaction services	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Sleep apnoea 1	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Sleep apnoea 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not sure	Yes
Smart bed 1	Yes	Not sure	Not sure	No	Yes	Yes	Not sure	No	Yes	No
Smart bed 2	Yes	Yes	Yes	No	Not sure	Not sure	Yes	Yes	Yes	Unknown
Vital data 1	Yes	No	No	No	Yes	N/A	Yes	Yes	Not sure	No
Vital data 2	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	No
Vital data 3	Yes	No	No	Yes	Yes	No	Not sure	No	N/A	No

Figure 7: Overview of the individual yes/no/unknown questions

Figure 7 shows the individual answers to the "yes/no/not sure" questions. Of the 13 questions, the first question concerned the classification of the devices therefore not shown in the matrix. In general, it can be deduced from the twelve questions that the participants who predominantly answer "yes" have implemented a higher degree of security measures for IT security than those who more frequently answer "no" or "not sure".

From the following product categories, no vendor/manufacturer participated in the survey:

Pillboxes and tableware, sleep monitoring, fall detection, reminder services, heated blankets, physical assistance, and rollators.

Overall, it can be summarised that the twelve respondents who participated in the survey considered IT security at varying degrees during the development. However, of the total of 52 personally invited participants, this is only one in four. The total of 84 manufacturers could not all be contacted for various reasons. 11 contacted manufacturers were reachable, but denied any interest in participating in the survey.

In fact, the survey does not prove to which extent the security measures have been implemented. The results obtained from the survey can be compared with the results from the physical examination of the devices. Furthermore, it is not comprehensible to what extent the participant was able to answer the questions in detail and in a qualified manner. Overall, the result is not representative due to the small number of participants as well as the lack of availability of manufacturers located in the USA or China, for example.

In conclusion, the identified devices are not entirely smart, i.e. in this case they provide particularly extensive functionalities or modalities related to the use of a connected device. The use of these products refers rather to basic assistance for everyday life, such as location/surveillance systems with alarm functions or walking aids that detect obstacles or measure and store vital data, but not to systems that offer a wide range of functionalities analogous to care robots or special interaction services.

3.3.4 Product selection for IT security assessment

When selecting products, a wide range of applications and different price segments had to be considered. From the available connected care products, a total of nine products were selected to be subjected to IT security assessments. Those were:

1. The mobile sleep apnoea therapy device with an integrated Bluetooth interface and the corresponding app, whereby the device can be controlled either via the touchpad on the device or via the app. A sleep apnoea therapy device is a medical device, but is often used in the home and care sector and was therefore considered.

2. The blood glucose monitoring system, which continuously measures the glucose level with a sensor that is applied percutaneously (i.e. piercing the skin). It can store, display, and evaluate the measured values using an app.

3. The connected nursing bed which transfers the status of its patient, e.g. position control, in real time and with activity history to an app.

Note: During the period of the online research (February-March 2019) the connected nursing bed was still advertised on the manufacturer's website. However, the product was no longer available at the time of intended purchase. No further information concerning the reasons can be provided.

4. The smart pillbox with a reminder function, as an optical or acoustic alarm, or a notification via app or SMS. The pills remain in their original packaging for hygienic reasons. The monitoring is realised via weight detection.

5. The Smartwatch with fall detection, localisation function and automatic emergency call initiation.

Note: According to the manufacturer, this is a pre-series product, which was still in the test phase at the time of the assessment.

6. The reminder service for senior citizens in the form of a tablet on which appointments, messages or photos etc. can be displayed.

7. The care ball, which interactively promotes the cognitive and motor skills of e.g. patients suffering from dementia.

Note: At the time of the IT security assessment, the care ball was still at prototype stage. The fundamentally open-minded development team explained that they are currently working on a production model. This would correspond optically, haptically and in the functional range to the prototype, however, in terms of information technology, it will be built on a completely new platform, including security functionalities. Since neither a documented IT security concept nor a technically identical pre-series device was available, an IT security assessment (in the context of this project) was not performed.

8. The smart heated blanket with a Bluetooth interface, whose temperature can be controlled via app.

9. The connected pulse oxymeter with a Bluetooth interface, which can store 100 measurements and transfer them to an app.

4 IT security assessment

4.1 Preliminary remarks

Since no binding or standardised procedure has been established for testing the IT security of medical or care equipment to date, the following general conditions and notes on the tests performed must be taken into account when evaluating the results.

4.1.1 Depth of inspection

The aim of the eCare project is to obtain a realistic estimate of the general IT security level of care equipment in the near future and at a manageable cost. On this basis, further need for action, such as further projects, targeted investigations or regulatory requirements, can then be identified, planned, and initiated.

In order to achieve the aim of the project, the available project budget was used to spread the tests very widely (examination of various communication connections, the associated apps, etc.) and to deliberately keep the test depth for each individual test aspect low. Thanks to the technical expertise of the security researchers employed, it was thus possible to ensure that a large number of "low-hanging fruits" were collected (investigations which provide meaningful results with a low expenditure of resources and are most likely to allow an estimate of the general IT security level).

However, it is important to note that the assessments are only random samples and snapshots and that the respective depth of testing is significantly lower than that of a full penetration test or a full IT security assessment according to a recognised standard, such as the Common Criteria evaluation, etc. It is assumed that any further vulnerabilities or security gaps that may exist were not uncovered during the course of the project's assessments. The results of the IT security assessment therefore only represent an upper limit of the IT security level achieved.

4.1.2 Black Box approach

The tests of all examined devices were carried out within the framework of a so-called "Black Box approach". This means that no insider information, such as security concepts, specifications or other previous knowledge was available. This procedure thus corresponds to that of an external attacker, who would rely on the device itself to extract all the necessary information. Therefore, the results cannot make any statement about the extent to which an insider or inside perpetrator could carry out further attacks, e.g. by exploiting conceptual weaknesses, existing backdoors or master passwords.

4.1.3 Exclusion of the functional evaluation

The work of this project focuses on the investigation of "security" (in the sense of protection against manipulation or unforeseen use). If the technologies used are capable of fulfilling the intended functions with the help of their "connectivity" in general, was not further investigated or evaluated in the course of the project. If one of the examined devices is a medical device in the formal sense, it can be assumed that a corresponding examination of the "safety" (in the sense of the intended use) has taken place. For products that are regarded as "care equipment" in the context of this project but are not formally medical devices, tests to ensure the advertised performance are not generally mandatory.

4.1.4 Reporting vulnerabilities to manufacturers

All identified vulnerabilities were communicated to the respective manufacturers prior to the publication of this report so that they had sufficient time to fix the identified vulnerabilities ("responsible disclosure"). However, at the time of publication of this report not all weaknesses may have been fully addressed.

4.2 Risk assessment methodology

For the analysis and evaluation of risks in information security in general, the possible amount of damage in the event of occurrence and the probability of occurrence of risk scenarios are determined or estimated. The risk level then results from a combination of these two values. The methodology for the security assessment of the evaluated products is described below. This can generally be used for the evaluation of IT security risks of IT-supported medical and care equipment, etc. Within the framework of this project, a metric for the quantitative calculation of a risk level was deliberately omitted (e.g. by multiplication of values), as no minimum security level to be achieved (also called "risk acceptance threshold") has been required by regulatory specifications so far. However, both regulators and manufacturers of such products may establish their own metrics to define their risk acceptance thresholds according to the categories described.

Since both the amount of damage and the probability of occurrence should be considered multidimensionally in the context of medical/care equipment, the following different aspects to determine the amount of damage and probability of occurrence are determined independently from each other.

4.2.1 Amount of damage

To determine the amount of damage, the concrete damage scenario, the number of people affected and the probability of detection of an attack or defect leading to the damage are estimated (see table 3 to table 5).

	Damage scenario
lower <- Amount of damage -> higher	Immediate severe injury or death.
	Negative effects on health.
	Treatment effectiveness reversed.
	Negative influence on therapy (limited treatment effectiveness) or impairment/failure of the intended function.
	Negative influence on therapy or impairment of the intended function is possible.
	Access to sensitive personal data (e.g. health data).
	Access to/manipulation of personal data.
	Access to/manipulation of data without personal reference.

Table 2: Assessment of the amount of damage - damage scenarios

	Number of people affected
lower <- Amount of damage -> higher	The influence goes beyond the user group.
	Affects all users / devices.
	Affects many users / devices.
	Affects a group of users / of devices.
	Affects only one user / one single device.

Table 3: Assessment of the amount of damage – number of people affected

	Probability of detection
lower <- Amount of damage -> higher	Cannot be detected.
	Can only be detected by IT security specialists / IT forensics.
	Can only be detected by a specialist / maintenance service.
	Only detected during specific checks.
	Detected during routine test / function checks.
	Deteced by user / operator after some time.
	Detected after a short time by user / operator.
	Immediately detected by user / operator.

Table 4: Assessment of the amount of damage – probability of detection

4.2.2 Probability of occurrence

In order to determine the probability of occurrence, the required access to the IT system and the characterisation of the attackers are estimated on the basis of the skills required to exploit a vulnerability or to perform an attack (see table 6 and table 7).

	Access to the IT system
lower <- Probability of occurrence -> higher	Access via internet.
	Access via internet, prior registration / authentication required.
	Wireless access, no authentication required (radio range).
	Wireless access, prior registration / authentication required.
	Access via IT network.
	Access via interface on the device.
	Access only possible via physical access and case opening.

Table 5: Assessment of the probability of occurrence - access to the IT system

	Characterisation of the attackers
lower <- Probability of occurrence -> higher	Secret Service
	IT security researchers
	Penetration testers
	Automated vulnerability scans
	Amateur hackers
	"Interested" user
	Possibility of random attack by users
	Possibility of random attack

Table 6: Assessment of the probability of occurrence – characterisation of the attackers

4.3 Results of the investigated products

For each of the products assessed, a detailed report of the respective investigations was prepared for the IT security assessment. In the following chapters, the results are summarised in anonymised form, the main results are examined in more detail and evaluated in the context of their intended use.

4.3.1 Mobile sleep apnoea therapy device

4.3.1.1 Description of the device

The use case for the investigated portable sleep apnoea therapy device is its use while travelling. Therefore, it is relatively small, light and equipped with a battery. Basically, the device can be set up locally and used without further connection. Furthermore, the therapy data can be exported in three ways (e.g. to monitor the therapy or transfer data to doctors, health insurance companies, etc.): via Bluetooth to the corresponding smartphone app, via USB to a PC and to a locally inserted SD card. Therapy data can be displayed, monitored, managed, and synchronised using the smartphone app and the PC application. A user account in the manufacturer’s cloud is required to use the app and the PC application.

4.3.1.2 Summary of the IT security assessments

As part of the IT security assessment, the communication between smartphone and app via Bluetooth, the app for the smartphone and the application for the PC were examined, respetively.

The connection via Bluetooth only takes place after successful pairing. After successful pairing, the Bluetooth communication is encrypted.

The smartphone synchronises the received therapy data with the cloud. The communication is encrypted, furthermore the app uses certificate pinning. A man-in-the-middle attack between the smartphone and the internet is therefore not successful. The source code of the smartphone application is obfuscated, whereas embedded strings were not obfuscated. The assessment has shown that the application uses stronger obfuscation than average, e.g. achieved bytools in the default settings. Due to the applied obfuscation technique, the scope of the application and the time limit of the project, a detailed analysis of the source code was not possible. It was discovered that usage data of the application is sent to a service provider in the USA. This is also mentioned in the terms of use.

The computer application also synchronises the received therapy data with the cloud. All communication is encrypted. The application for the computer is available for Windows and MacOS and can be downloaded from the manufacturer's website. It is a Java application that is partially obfuscated. When analysing the source code, a number of functions could be identified, that can send various commands to the device via USB. Those can read and change data from the device. No authentication is required. The application supports a number of devices of the product family and thus includes functions that are not used by the sleep apnoea therapy device. Among other things, one function could be identified, which allows to change the serial number of the device. If the serial number is changed, no data can be exchanged with the application or with the smartphone app anymore, because the serial number is permanently stored in the account and is checked when the connection is established. It can also be queried via the PC application (structured) whether an e-mail address is known in the system or not. This makes it possible to generate lists with valid serial numbers and existing e-mail addresses. The e-mail address and serial number are sufficient to change an account’s password. The user will not be notified that his password has been changed.

4.3.1.3 Conclusion on the device

The communication between the ventilator and smartphone as well as the communication from the smartphone to the cloud can be considered as state-of–the-art. The Bluetooth communication is encrypted and the app uses certificate pinning. The obfuscation techniques used are effective in making a targeted search for vulnerabilities more difficult.

However, the system can be attacked via the USB interface and the corresponding application for the computer. This makes it possible for an attacker with *penetration tester* skills to stop the synchronisation of the data with the smartphone or the computer and to enumerate user names and serial numbers[3]. With the help of this data, it is possible to change the passwords of the accounts, to take them over unnoticed and to *access all stored therapy data*. This vulnerability affects *all users with a corresponding cloud account*. Enumeration can (if at all) only be discovered by the *IT experts of the backend system*, but *not by individual users*.

4.3.2 Blood glucose monitoring system

4.3.2.1 Description of the device

The examined blood glucose monitoring system consists of several components: A sensor in the form of a plaster with a fine measuring needle is stuck to the skin for continuous measurements of the glucose level directly under the skin. A transmitter sends the measured data via Bluetooth to the corresponding receiver or a smartphone, which displays the blood sugar values in the form of continuous measurement curves. With the help of the smartphone app (or via the associated receiver using USB and a computer application), the data can be sent to a cloud portal, which allows for better analyses, for example. In addition, further apps are offered, which enable the evaluation and forwarding of cloud data to third parties. Both on the user's devices and on those of the "followers", individual warnings and alarms can be defined when values exceed or fall below specified parameters. For example, parents are able to continuously monitor their children's blood sugar levels and inform the teachers at school if urgent action is required.

4.3.2.2 Summary of the IT security assessments

As part of the IT security assessment, the connections via Bluetooth and Wi-Fi, as well as two of the smartphone apps were examined.

The smartphone app or receiver has to be first "paired" with the transmitter via Bluetooth. The connection is then used to regularly transmit the blood sugar values to the smartphone or receiver. The connection is encrypted. The transmitter uses the pairing mechanism "Just Works". Since no out-of-band pairing is used and the "Secure Connection" and "MITM" (man-in-the-Middle) flags are not set, the connection does not provide protection against man-in-the-middle attacks. Since in the mechanism the encryption key is derived from a known code ("000000"), the key used can be calculated and thus the communication can be decrypted.

The connections of the two examined apps to the cloud are encrypted, respectively. Both apps use certificate pinning. A man-in-the-middle attack between one of the two apps and the internet can still be partially successful, since the app uses certificate pinning only after login. It is therefore possible to record the login and thus access the login data. For a successful attack, however, the certificate of the "malicious Certification

[3] Account/User enumeration: Structured, possibly automated procedure for obtaining information about the validity of credentials.

Authority (CA)" has to be installed first on the smartphone, which considerably increases the complexity of the attack.

There is no effective code obfuscation, which simplifies reverse engineering of the application. Both apps only request necessary Android permissions. One app uses reading and writing from and to external memory to export reports on the progress of measurements. However, this allows other apps to access the data, which is critical because the data is not removed from the external storage. Both apps use simple mechanisms to detect rooted devices (root detection). Since not every root method is detected with the examinations performed and since the apps start regardless of the result of the root check, it can be assumed that the root detection is mainly used for error reports.

4.3.2.3 Conclusion on the device

The Bluetooth connection is encrypted and the apps use certificate pinning most of the time. In the case of the app, in which certificate pinning is only used after login, an attacker with *access to network traffic* with a malicious CA *via the internet* (at least *penetration tester level*) can *access the login data* and consequently *the health data of a user without being noticed*. The apps are not obfuscated, which simplifies reverse engineering of the applications.

One of the apps stores the generated reports in the external memory of the device and does not delete them even after they have been transferred to an e-mail client, for example. This allows other (manipulated) apps that have access to the external storage to access these reports including the *health data*. This access can only be *detected by IT forensics*. A targeted, successful attack requires a high attacker level (at least *penetration tester level*). The *victim group* must have both apps installed.

4.3.3 Smart pillbox

4.3.3.1 Description of the device

The smart pillbox examined uses a built-in sensor to detect when medication is added or removed. Medication can be set up, monitored, and evaluated via a smartphone app (e.g. intervals between doses of each medication, including reminders and notifications of missed doses). The pillbox allows connections via Wi-Fi to the provider’s cloud and is configured via Bluetooth using a smartphone. Relatives can use another app to check if the medication has been taken accordingly.

4.3.3.2 Summary of the IT security assessments

As part of the IT security assessment, the connections via Bluetooth and Wi-Fi, as well as the smartphone app were examined.

The smartphone app can establish a direct connection with the pillbox via Bluetooth. This connection is used to perform the initial configuration of the pillbox. After initialisation, the Bluetooth connection is no longer required. The further communication between the pillbox and the smartphone app is handled by the cloud. Bluetooth connections between app and pillbox are established without previous pairing. Therefore, no encryption of data at the transport level or secure authentication between device and the user's smartphone is possible. Bluetooth is permanently activated on the pillbox so that every smartphone in close proximity can connect to the corresponding app and configure the pillbox without further authentication. During setup, the API URL is set via Bluetooth. An attacker can change this by intercepting and manipulating the command or through a replay attack. During the tests carried out, the pillbox could no longer communicate with the cloud after the API URL was changed and thus no longer fulfil its intended function. The Wi-Fi is also configured during setup. The user selects a Wi-Fi network to which the pillbox is connected via the Bluetooth-connected app. If the selected Wi-Fi network is protected by a password, this password must be entered via the app. The app then sends the password unencrypted via Bluetooth to the pillbox so that it can be accessed by an attacker in range. The Wi-Fi to be used can also be changed via Bluetooth. If a new Wi-Fi is set up which does not require a password, the pillbox sends the password of the last configured Wi-Fi network back to the app via Bluetooth. Due to the missing authentication of the Bluetooth connection, an attacker can thus easily configure a new Wi-Fi network without a password and obtain the password of the previously configured Wi-Fi from the pillbox. This allows the attacker to establish a connection to the previously configured Wi-Fi network.

After the pillbox is initialised via app, the pillbox establishes a connection to the cloud. This connection is used to exchange all data between the app and the pillbox. A man-in-the-middle attack between the device and the internet cannot be successfully executed without further effort. The pillbox does not connect to the server because the connection is protected via https and the device does not trust the CA of the man-in-the-middle system.

Similar to the pillbox, the app establishes an https connection to the cloud in order to transmit data to or receive data from the pillbox. Since no effective obfuscation is used in the app code, reverse engineering is simplified. The app requires a number of Android permissions, including five permissions which Android classifies as "dangerous". During dynamic tests of the app, only one of those permissions was actually requested. No other active functionality could be identified. For this reason, it can be assumed that the permission requests originate from the use of third-party libraries, but the permissions are not used as long as the implemented app does not start a corresponding function. The app includes an option for root detection, which is only used when a user wants to submit a bug or a suggestion for improvement. However, the possibilities of root detection are limited and are not able to reliably detect a rooted device. During tests with a rooted device the method was not able to identify the device as such. Although no certificate pinning is used (which only accepts one CA), the examinations have shown that the app does verify certificates and at least restricts them to those CAs that are stored on the device used and does not establish any further connections.

4.3.3.3 Conclusion on the device

The security assessment carried out has shown that the product exhibits considerable weaknesses regarding the Bluetooth connection. The vulnerabilities can be used by an attacker (*amateur hacker*) *in range* of the Bluetooth receiver to *eavesdrop* on the device (such as *health data*), *disable* the device and *gain access to the user's Wi-Fi*.

The app uses established security procedures regarding protection. However, these are not fully implemented consistently and therefore show some medium vulnerabilities. A final evaluation of those is not possible without further examination of the API and backend systems.

4.3.4 Emergency call watch with fall detection

4.3.4.1 Description of the device

The examined "smart" emergency call watch with fall detection is mainly based on a conventional smartwatch. If the person wearing the watch falls, a countdown is initiated and after the countdown has expired, an emergency call is made via GSM to a previously defined location (e.g. call to the manufacturer's emergency call centre or via SMS to an emergency contact). The emergency call can also be triggered manually. In case of an emergency call, the position is determined via GPS and also forwarded. The watch can also request regular vital signs from the wearer. The vital signs can then be viewed, for example by relatives using another smartphone app. The app displays requested and confirmed life signs with the corresponding date and time.

4.3.4.2 Summary of the IT security assessments

As part of the IT security assessment, the "smart" watch app as well as the smartphone app were examined. There is no direct communication between smartphone and watch. This is performed via the cloud of the provider.

A first look at the device showed the Android version used and its patch level. This was Android 7.1.1 with the security updates of March 01, 2018. At the time of delivery, the installed patch level has already been one year old. Some functions of the clock can be controlled via SMS. For some commands, the user does not receive any information about their execution. The SMS functions are shown in the following table.

Function	Description
Callback	A "sign of life" is requested.
Position	Here, the location of the device is transmitted to the SMS sender. The user of the clock is not being notified of this.
Update	It was not possible in the context of this review to determine exactly how this mechanism works in detail. However, it seems that only configuration updates are possible and not an update of the entire application.
Mobile (on/off)	Mobile data is activated or deactivated.
Wifi (on/off)	The Wi-Fi module of the watch is activated or deactivated.
Unlock	The device will unlock. Normally, gestures on the watch cannot be used and the settings menu cannot be accessed. With the "Unlock" command this lock is removed and the watch can be operated like a normal Smartwatch.
Reboot	The device is restarted remotely.
Clear Data	The user data of the application will probably be deleted.

Table 7: SMS functions of the emergency call watch

A security code is required for communication via SMS. It is calculated from the IMEI of the watch. The algorithm for calculating the security codes was determined by reverse engineering the app. This was made easier due to the slight obfuscation of the programme code. If an invalid security code is sent, the watch sends an SMS back, stating that the security code could not be processed. This would allow the security code, which can have a maximum of 135 different values, to be guessed by trial and error if the IMEI is unknown.

The ADB interface via USB is activated by default. To establish a connection with the interface, a confirmation must be made on the watch. This can be achieved in two ways: On the one hand, entries can still be made on the screen directly after a restart of the watch, and on the other hand the device can also be unlocked accordingly via the SMS command "Unlock". With the help of the ADB shell, root privileges can be obtained. The root account is not password-protected, so that only the command "su" is necessary for an extension of rights. With an active root account, an attacker has full control over the device and can for example install an application that sends arbitrary data from the device to a system controlled by the attacker. The attacker could also access the microphone and eavesdrop on the wearer of the watch unnoticed.

The app of the watch uses a simple obfuscation. This means, class, method and variable names cannot be restored. The names have been replaced by combinations of lower case letters, which means that the names alone no longer allow any conclusions on the functionality. Strings hard-coded into the apps are not obfuscated. The app implements trust managers that accept any certificate without verification. An attacker can thus perform a man-in-the-middle attack by presenting any certificate to the app.

The smartphone app communicates with the manufacturer's cloud via an API. For communication with the API, the http protocol is used, which does not use transport encryption. Due to the lack of transport encryption, the communication between smartphone app and cloud can be eavesdropped and modified. For example, signs of life can be manipulated or suppressed in this way. Authentication is based on the IMEI and another security code. The calculation for the security code of the API access is more complex than that of the SMS security code and can take a maximum of 4536 values. The calculation could also be taken from the reconstructed source code.

4.3.4.3 Conclusion on the device

The IT security assessment has shown that the emergency call watch system is affected by several vulnerabilities. Attackers (*amateur hackers*) with knowledge of the phone number and the IMEI *of the device* (e.g. relatives of the user) or *several devices* (e.g. possible middlemen) are able to query the *position of the wearer* (continuously) *via SMS*. The query *is unnoticeable for the user*. Physical proximity is not required for a successful attack at any time.

If, in addition, *one-time physical access* to the watch is made possible, an attacker (*amateur hacker to penetration tester*) can easily gain root rights *for a device* and, by using malicious programmes or other forms of manipulation, access *to all data of the wearer collected/produced by the watch* can be *obtained unnoticed* or the wearer can be directly *intercepted*.

The implemented security measures do not offer any substantial protection against "attacks", but at most protect against inadvertent entries.

4.3.5 Tablet for senior citizens

4.3.5.1 Description of the device

The tablet is advertised as a watch with a "special" calendar and reminder function for senior citizens. The device is a conventional Android tablet with the "special" watch and calendar function as an app. The calendar is characterised by the fact that it can be filled with information or images from third parties, such as relatives or nursing staff, via cloud. The pre-installed app starts automatically, so the tablet can no longer be used as a classic tablet. The calendar and photo functions are part of a subscription and can only be used after receiving a username and password from the manufacturer. The watch is the only function that is also available without a subscription. The purchase of the device includes a free half-year subscription.

4.3.5.2 Summary of the IT security assessments

Within the scope of the assessments, the "special" app, the underlying Android, as well as the communication with the manufacturer’s cloud regarding entering calendar entries and photos were to be examined.

Note: The device could not be fully evaluated because the essential calendar and photo functions must first be enabled by the manufacturer. The activation code required for this was requested from the manufacturer according to his specifications, but was not delivered during the evaluation period.

In the following, the findings about the app, the underlying Android and the communication with the cloud, which could be assessed without activation, are described.

At a first look at the device, the used Android version and its patch level were determined. This was Android 7.1.2 with the security updates from March 05, 2018. At the time of delivery, the installed patch was already one year old.

The tablet requires an active Wi-Fi connection. To set it up, the settings of Android, which are normally not accessible, are used. From the Wi-Fi settings menu, one can navigate to the general Android settings, allowing to configure any desired settings. For example, the debug interface (ADB) can be activated to access the device via USB. It was also possible to use the normal Android launcher, in contrast to the system launcher of the app. This makes it possible to use the tablet as a conventional Android tablet, with all the associated risks for the data on the device.

During the brief evaluation of the application, it was found that the communication with the API is unencrypted. With the help of the extracted source code, the unencrypted transmission of login data could be confirmed again. Username and password are sent as part of the URL. Thus, the data is not only sent unencrypted, but is also potentially logged by the proxies used as well as by the target web server, since accessed URLs are usually written to log files. It could be detected that the app processes used passwords before sending them with the hash algorithm "MD5". It sends the corresponding hash value during authentication instead of the password in plain text. MD5 has been considered breached for a long time and is no longer classified as "secure". Sending the hash value of the password instead of the plain text password also does not increase the security of the authentication procedure, since an attacker could use a hash value intercepted during transmission for authentication without knowing the plain text password. The use of MD5 during authentication also suggests that the passwords in the backend are also stored as MD5-hash values. If the backend is compromised and the stored passwords are obtained, MD5 offers only insufficient protection against attempts to guess the plain text passwords with appropriate tools.

A more comprehensive evaluation of the app could not be performed due to the fact that the device was not activated.

4.3.5.3 Conclusion on the device

A meaningful and resilient evaluation of the IT security is not possible on the basis of the evaluations carried out, taking into account the missing activation code.

The findings on the unencrypted data transmission between app and API, where an attacker could eavesdrop, record and modify the communication, as well as the use of the MD5-hash procedure, which has long been considered insecure, suggest that no comprehensive IT security concept has been implemented and that more in-depth evaluations of IT security would reveal additional vulnerabilities.

4.3.6 Pulse oxymeter

4.3.6.1 Description of the device

The evaluated pulse oxymeter is a small device in the form of a clip that is placed on the finger. With the help of a light source and a light sensor, the oxygen level in the blood as well as the pulse is determined via the light absorption of the blood. The device has a built-in display. It can also transfer the measured values via Bluetooth to a smartphone with a corresponding app. The pulse oxymeter belongs to a full range of health management products that can be synchronised and connected via the app and the cloud of the provider. After logging in to the online portal, the data collected in the cloud is also accessible via web browser, i.e. without having to directly use the app.

The device is advertised with a security label "data protection and data security" which, according to information on the product's website, refers to the web application of the online portal. The pure reference to the online portal is not apparent from the information on the product packaging or the enclosed user instructions.

4.3.6.2 Summary of the IT security assessments

As part of the IT security assessments, the connection via Bluetooth, the communication between the app and the cloud, the app itself and the online portal were evaluated.

The pulse oxymeter uses Bluetooth without pairing. Therefore, no encryption of data at the transport level or secure authentication between device and the user's smartphone is possible. As soon as a connection to the device is established, the data is transmitted unencrypted after the "send" command. The source code of the included app is not obfuscated and can be easily converted back into readable code. With the help of the source code and due to the missing transport encryption of the Bluetooth communication, individual data packets can be analysed easily, their structure can be examined and the data contained therein can be accessed. Additionally, the pulse values, oxygen saturation, and time stamps sent to the app can be changed. However, these are not changed on the device itself. With the next synchronisation between the device and the app, the correct data will be delivered subsequently. Besides the possibility to manipulate the values that the device sends to the app, it is also possible to manipulate the time setting inside the device itself.

The application on the smartphone communicates via https with the cloud. No certificate pinning is used here, making a man-in-the-middle attack easily possible. The synchronisation between app and cloud is only carried out if it is actively initiated by the user. In this case, the man-in-the-middle has full control over the data exchanged between smartphone and cloud.

The app does not use source code obfuscation, which makes it possible to decode the Bluetooth communication efficiently. Furthermore, the app does not use certificate pinning. This makes it possible to position oneself as a man-in-the-middle in cloud communication and to monitor and analyse it. The app requests eight rights, which are classified as "dangerous" by Android and which are only granted since Android 6.0 (API Level 23) after the user's approval and which cannot be obtained implicitly by installing the app. One of the rights requested is "WRITE_EXTERNAL_STORAGE". This feature can be traced back to report generation, that can be run from the app to sent reports on the collected data, e.g. via e-mail. The application thus stores sensitive data on the external storage area of the device used, making the data readable by all apps using the right "READ_EXTERNAL_STORAGE". The app does not implement certificate pinning, which allows all CAs stored on the device to be trusted. If an attacker can issue a valid certificate for the application using a compromised CA certificate, this would allow requests to be redirected to servers under the control of the attacker. When analysing the code of the application, a firmware update function could be identified. The class "FtpFirmware" is used to download the new firmware via FTP. FTP itself does not provide encryption, so all files are transferred in plain text. In addition, the access data for the FTP server used could be identified in the application, since the access data is programmed into the applications in plain text. Due to the missing encryption, an attacker can read and modify the data traffic. The checksum, which is provided by the ".ini"-file, does not provide any additional security, since the ".ini"-file can also be manipulated during the transfer. In addition, an attacker can redirect the requests to his own malicious FTP server, since without encryption, no certificate check is carried out and the client cannot verify the identity of the server.

When creating a new account on the online portal, the http response contains an activation link. It can be used to activate the account. An attacker can thus create accounts for any e-mail address without having control over the e-mail accounts. Via an http-post it is possible to check if an entered e-mail already exists in the system. Furthermore, a password reset for the online portal login can be requested for an existing account without further verification or authentication. The http-response contains a link, with which the password of the account can be changed in an unauthorised way. Consequently, any account of any user can be taken over.

4.3.6.3 Conclusion on the device

The IT security assessment has shown that the pulse oxymeter is susceptible to several vulnerabilities that could compromise the integrity, confidentiality, and availability of the device, the corresponding app and the online portal. As the data collected and managed by the device are health data, the impairment of confidentiality and integrity is considered particularly critical.

All *user* data (incl. *health data*) transmitted unencrypted via Bluetooth can be *accessed unnoticed* by an attacker with the capabilities of an *amateur hacker in range* without much effort and can be manipulated *until the user discovers* implausible values. If the measurement is used to determine therapeutic measures, e.g. when taking medication, and if the data is changed within a plausible range, the manipulation can *only be noticed if it is properly examined* and can at least remove the *intended function of correctly measuring* pulse or oxygen saturation. *A negative influence on the therapy* up to *negative health effects* cannot be generally excluded in the case of effects on a related medication.

The app shows several vulnerabilities which can lead to manipulation of the communication between the app and the cloud and thus to *health data being accessed*. The scenario concerning another malicious app could affect a *group of users* who use both apps. Due to the complexity of a successful attack and a comparatively small "prey", this scenario is most likely to be attributed to *IT security researchers*. Attacks of this kind can occur *via the internet* without direct physical access. The probability of detection is considered low and can only be detected *by an IT security specialist or forensic scientist*.

The access to e.g. *health data* stored in the online portal basically affects *all online portal users* and can be carried out by an *amateur hacker via the internet* without much effort. Although the attack can be *noticed by the users quickly*, all data would have already been successfully accessed at this point.

5 Project conclusion

5.1 Market analysis

A list of the identified care product types in this study is given in chapter **3.1.3**, the number of products found for each category in chapter **3.2.2**. However, since there is no superior system for the classification of care products (contrary to medical devices), the definition of the types is subjective to a large extent.

The functional scope of connectivity depends on the type of product and also on each individual product. There are products for which connectivity is only an additional function (e.g. storage of measured values in the cloud for statistical purposes), i.e. the product also functions without connectivity, and other products for which connectivity is a central component of the function (e.g. fall detection).

In the survey, the manufacturers declared more measures as implemented than the authors would have suspected based on their experience. This can have two reasons: On the one hand, it is likely that manufacturers, who at least to some extent considered the topic of IT security during development, participated in the survey. On the other hand, the authors assume that insufficiently implemented measures also tend to be answered with yes, i.e. implemented. So the assumption remains that IT security is in fact addressed to a lesser extent than the survey shows.

The market analysis has shown that care product connectivity is certainly an issue. However, connectivity today still solves isolated issues, such as remote control of a device or the storage of data from a device for statistical purposes. Both full connectivity and connectivity between individual devices are still quite rare at present. The "nursing robots" discussed in the media can probably not be expected for several years.

5.2 Status quo of IT security

In the context of this project a total of six randomly selected connected care devices currently available on the market were analysed with regard to their IT security features. The selected devices covered a broad spectrum in terms of function, price, interfaces and the size of their manufacturers. In conclusion, taking into account the particularly high level of protection required for health data, the IT security level found can be assessed as poor to very poor. This can be explained, among other things, by the fact that medium to severe vulnerabilities were detected in all examined devices. In addition, it must be taken into account that, due to the general conditions of the project, the depth of testing can definitely be described as low and by no means corresponds to a full penetration test or a security evaluation. The vulnerabilities found suggest that none of the devices examined, including the associated apps or cloud services, has previously been subjected to a professional penetration test, since all the vulnerabilities found would also have been discovered (assuming that the manufacturers did not treat all risks with acceptance). It can also be concluded that information security management was of secondary importance in the development of the devices, as otherwise, for example through ISO 27001, an independent audit of IT security would have been demanded (provided that adequate IT security of the devices and effective protection of health data were defined as objectives of information security management). It can also be concluded that available guidelines for the development of secure, connected medical devices, such as the BSI recommendation on "Cyber Security Requirements for Network-Connected Medical Devices" (BSI-CS 132)[4], the "Guidance on Cybersecurity for medical devices" (MDCG 2019-16)[5] or "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices"[6] and "Postmarket Management of Cybersecurity in Medical Devices"[7] by the FDA[8] have

[4] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_132.pdf
[5] https://ec.europa.eu/docsroom/documents/38941
[6] https://www.fda.gov/media/86174/download
[7] https://www.fda.gov/media/95862/download
[8] FDA = U. S. Food an Drug Administration

not been considered sufficiently. Positive is the fact that most of the manufacturers of the examined products basically already use various IT security measures, such as encryption or authentication mechanisms.

In particular for care devices, which are not formally classified as medical devices, but also for the more strictly regulated medical devices, no concrete measures to increase or ensure and test sufficient cybersecurity have been required by the regulatory authorities to date. The examinations show that the voluntarily achieved security level offers only insufficient security to a large extent.

When qualitatively assessing the security situation based on the project results, it must be taken into account that only the products themselves, including their apps, but not the corresponding backend systems, were examined within the scope of the presented assessments. Since vulnerabilities found in these systems usually affect large user groups immediately and due to the fact that they can be accessed directly via the internet, it is highly recommended that, based on the negative results of the devices, more in-depth assessments of the backend systems should be carried out.