HEALTH DATA FOR SALE?

Consumer protection and privacy in blood pressure monitors and blood glucose meters for home use

28.09.2017

FORBRUKERRÅDET

Innhold

Summary

In an investigation into blood pressure monitors and blood glucose meters for home use, the Norwegian Consumer Council has looked at devices that connect to the internet via associated mobile applications. During the course of the investigation the Consumer Council identified a number of faults with the devices and services with regard to consumer protection and privacy. Such devices, and especially blood glucose meters, may pose significant privacy risks since information about the use of the device alone can reveal a great deal about an individual's state of health. When a device that collects health data connects to the internet, it may also compromise the user's control over their own data. Many of the devices examined by the Consumer Council automatically upload readings to cloud servers, while some also transmit data to companies in East Asia and North America without notifying the user. Many of the services also allow health data to be shared via email, which is not a secure channel for such information.

The Consumer Council notes that the terms of use for these services are long and indecipherable. For instance, it is unclear how personal data may be used, and all of the suppliers are free to amend their terms of use without notifying the user. Just by reading the terms of use it becomes clear that consumer protection and privacy rights are being compromised.

Introduction

Consumers are being increasingly exposed to new digital health tools. This is an evolving market in which new technologies enable users to perform health tests at home without having to see a doctor. When these tools go digital and connect to the internet it also means that health data is uploaded and stored on cloud servers. The Consumer Council's concern in this regard is that users must remain in control of their own health data. Users must be given health tools that give accurate readings, the terms of use must provide adequate information, and providers must not misuse and/or resell health data.

Home testing devices are sold over the counter by pharmacies and electronics retailers as well as on a number of Norwegian websites. As part of its e-health programme, the Consumer Council has opted to investigate devices available on the Norwegian market, some of which are digital and linked to associated mobile applications. Among these devices, we have chosen to focus on blood pressure monitors and blood glucose meters. The former can be useful for consumers who need to keep an eye on their blood pressure on a regular basis without having to see their GP in order to take a reading. Blood glucose meters are used by many diabetics, allowing them to keep track of their glucose levels, food intake etc.

The Consumer Council has looked at 22 devices – 12 blood pressure monitors and 10 blood glucose meters. Four of the blood pressure monitors and three of the blood glucose meters are used in combination with a smartphone and come with associated apps. This enables many of the devices to offer added functionality such as cloud storage, visualisation of results and other additional functions, including digital reporting to the user's GP. Some of the devices without associated apps come with the option to upload data to a computer, although this function appears to be an auxiliary function for those taking a special interest. This report looks more closely at the seven devices with associated apps, which we consider to promote the app connection as a key feature of the product.[1]

The Consumer Council has previously investigated mobile applications (Appfail)[2] and internet-connected activity wristbands and toys (Toyfail).[3] We reviewed the terms of use and carried out technical tests of the products. Our review found major weaknesses in consumer protection and privacy amongst market-leading products and services.

Digital health products such as blood pressure monitors and blood glucose meters process health data, which is highly sensitive personal information. It is also information that can be commercially attractive to someone who wishes to use it for advertising purposes, for instance. The Consumer Council therefore decided to look at how consumer protection and privacy are safeguarded in apps linked to home testing devices. We also conducted a functionality test of all the products in order to analyse user-friendliness and accuracy. Consultancy firm Bouvet also conducted a technical test of the products with app connections. A summary of the technical tests has been included as an appendix to this report.[4]

The products

The following blood pressure monitors with associated apps were analysed: Andersson BDR 1.0 with the MedM Health app, QardioArm with the Qardio Heart Health app, iHealth BP7 with the iHealth MyVitals app, and Withings WPM02 with the Withings Health Mate app. As for blood glucose meters, the Consumer Council tested the following products: 2in1 with the 2in1 Smart app, Contour Next One with the Contour Diabetes app (NO), and iHealth BG5 with the iHealth Gluco-Smart app. All products were either purchased from a Norwegian retailer or ordered from a website aimed at Norwegian consumers.

[1] Partly because of information on the packaging
[2] https://www.forbrukerradet.no/appfail/
[3] https://www.forbrukerradet.no/tingenes-internett/
[4] *Investigation of privacy and security issues with internet connected health gadgets*

Product	Andersson BDR 1.0	QardioArm	iHealth BP7	Withings WMP02	2in1 Smart	Contour Next One	iHealth BG5
App	MedM Health	Qardio Heart Health	iHealth MyVitals	Withings Health Mate (replaced by Nokia Health Mate)	2in1 Smart	Contour Diabetes (NO)	iHealth Gluco-Smart
Function	Blood pressure monitor	Blood pressure monitor	Blood pressure monitor	Blood pressure monitor	Blood glucose meter	Blood glucose meter	Blood glucose meter

The MedM Health, Qardio Heart Health, iHealth MyVitals and Withings Health Mate apps are all part of a wider ecosystem of products and services, and the devices we tested are only linked to one or a few of the functions offered by the app. The 2in1 Smart, Contour Diabetes and iHealth Gluco-Smart apps are designed for and can only be used with the devices in question or with a series of blood glucose meters from the same manufacturer. All the apps are available on Android and iOS smartphones, and the technical test was carried out with both operating systems.

The analysis of the terms of use and the technical tests were carried out in May 2017.

Method

The terms of use were analysed by locating and downloading the terms of service/terms of use/EULA and the privacy policies/statements for the relevant apps. This process was straightforward in most cases. With three exceptions,[5] the documents could be accessed when downloading the apps from Google Play and App Store.

In the case of the 2in1, iHealth MyVitals and iHealth Gluco-Smart apps, we have not been able to find any relevant terms of use on the internet. The 2in1 app is not internet-connected, which may explain the absence of both terms of use and privacy policy. With regard to the iHealth apps, only the privacy policy is available online, while the terms of use that the app distributors (e.g. Google Play and App Store) link to only seem to apply to the website for the service. The terms of use for the actual apps are only accessible when launching the apps, and they are identical for both services. This poses a problem, because it means that users are most likely not presented with the terms of use until after they have purchased the physical product.

[5] 2in1, iHealth MyVitals and iHealth Gluco-Smart

On the basis of existing privacy and consumer legislation, the Consumer Council drew up a series of general requirements[6] as well as more specific criteria for use in its analysis. In light of these criteria, the terms of use for the apps have been evaluated according to the traffic light principle whereby green means the criterion has been fulfilled, red means it has not been fulfilled, and amber means it is not clear whether the service fulfils the criterion.

Security is key since health data constitutes sensitive personal information. We have therefore looked more closely at the extent to which personal data is transmitted by the apps, especially to third parties. The technical test involved a series of data flow analyses to establish where and when data is transmitted from the services.

Personal data

Personal data is information or evaluations that can be linked to you personally and which can therefore be used to identify you. Provisions on the processing of personal data can be found in the Personal Data Act, which is there to safeguard fundamental privacy principles. The essence of these privacy principles is that everyone is entitled to have their private sphere and personal integrity protected and for every individual to have the right to decide over their own personal data.[7]

Information about health matters constitutes sensitive personal data under the law, and there are specific requirements in place for the processing of such information above and beyond the general rules on processing personal data, which must also be observed. Blood pressure and blood glucose data is information about health matters and therefore constitutes personal data under the law if the data can be used to identify you. Blood glucose meters are only used by diabetics, which means that using such devices (with an associated app) reveals information about the user's diagnosis.

If it were to get into the wrong hands, information about the health of individuals can have serious negative consequences for that person. In addition, commercial third parties may also wish to access such data. For examples, insurance companies can use it to perform risks analyses and set prices,[8] while others may want to use the information for targeted advertising. Suppliers of app services must therefore ensure that such data is processed responsibly.

---

[6] https://www.forbrukerradet.no/siste-nytt/forbrukernes-10-krav-til-digitale-tjenester/

[7] https://www.datatilsynet.no/om-personvern/personvernprinsippene/

[8] Such practices are not in use in Norway at this time, but similar methods have been adopted for car insurance. https://www.dinside.no/okonomi/na-kommer-bilforsikringene-med-kjorestil-analyser/65347994

During the technical test, Bouvet observed that third parties were receiving information about the use of blood glucose meters.[9] In other words, a third party learns that the app user has diabetes and can use this information for profiling and potentially for discriminatory purposes. Offers and prices may be adjusted based on that individual's digital profile, for instance.

The apps provide different explanations of what information they collect and class as personal data. Only Withings is clear about what it deems to be personal data:

> *Personal data (hereinafter "Personal Data") any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. (Withings Terms of Service)*

When you give your consent to terms of use and privacy policies you permit the service provider to collect and process sensitive personal data. A study carried out by the Norwegian Board of Technology and the Data Protection Authority found that while many Norwegians are willing to share exercise data for research purposes, many more are sceptical about sharing the same information with insurance companies.[10] It is important, therefore, that suppliers are clear about what the service considers to be personal data, how this data is processed, and in which contexts the data may be used.

Consent

Before you can start using a digital service, you have to consent to its terms of use and privacy policy. Such consent is often given when you open the app for the first time or when you create a user account. The service will typically ask you whether you accept the terms of use and/or the privacy policy. Your acceptance is required in order to start using the service. The user must give their consent in order for the service to be able to legally collect and process their personal data. The length and frequently convoluted language of these terms of use mean that very few people actually review or read the terms before clicking "accept".

The user's consent must be informed and be given explicitly and freely. The length of the terms analysed in this study varied between 4,931 and 7,229

[9] *Investigation of privacy and security issues with internet connected health gadgets*, item 5.7

[10] https://teknologiradet.no/wp-content/uploads/sites/19/2017/01/Personverndagen-2017_web_korrigert-20170203.pdf page 33

words. The average word count stands at 6,653 – equivalent to around 14 A4 pages of standard-sized text.[11]

For consent to be considered informed, any changes to the terms of use must be announced in advance. Only then can the user familiarise themselves with the new terms and cancel the service if they so decide. None of the services investigated promises to notify the user before changing its terms of use. In practice this means that the service can make significant changes to the user's rights without their being aware of it. Making unilateral changes to the terms of use may be in breach of the directive on unfair terms in consumer contracts.[12] For example, iHealth's terms of service asks the user to check the terms from time to time rather than actively notify the user of any changes:

> *"iHealth reserves the right to make changes to these Terms and Conditions, including the Privacy Policy, at any time. Please check these Terms and Conditions and the Privacy Policy when you use the Application to ensure that you are aware of any changes." (iHealth terms of service)*

	Andersson	QardioArm	iHealth BP7	Withings	2in1	Contour	iHealth BG5
I will be notified about changes in the terms.	✗	✗	✗	✗	n/a	✗	✗

In late July 2017 (after the Consumer Council had completed the analysis of the terms of use) the Withings Health Mate app was replaced by Nokia Health Mate following Nokia's acquisition of Withings. The takeover resulted in an automatic update of the app and new terms of use. The automatic update did not disclose the app's new terms of use or request renewed consent. The changes were announced by email, but that email was sent two days after the new terms of use had come into force.

The Consumer Council has not analysed the new Nokia Health Mate terms of use in depth. We also note that the new terms have resulted in at least one significant change in that Nokia now reserves the right to use personal data for

[11] *In comparison, the average word count of the terms of 20 mobile apps analysed by the Consumer Council for the Appfail project was 5,700. The terms of use of the blood pressure monitors and blood glucose meters are thus relatively wordy.* Scope and presentation will also be considered when assessing whether the terms of use are unfair under the directive on unfair terms in consumer contracts.

[12] http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A31993L0013

marketing purposes. Withings' privacy policy included a promise never to use the users' personal data without obtaining their prior consent:

> *We never work with your data when it identifies you unless you have given us your consent, for example in order to resolve a problem that you have pointed out to us when you contact our customer service department. (Withings Privacy Policy)*

Nokia Health Mate takes a more liberal approach to the use of personal data:

> ***We may use your personal data to develop and manage our products**, services, customer care, **sales and marketing**. We may combine personal data collected in connection with your use of a particular Nokia product and/or service with other personal data we may have about you, unless such personal data was collected for a different purpose.*

It continues:

> *We may contact you to inform you of new products, services or promotions we may offer and to conduct market research when we have your consent or it is otherwise allowed. **We may use your personal data to personalize our offering and to provide you with more relevant services**, for example, to make recommendations and to display customized content and advertising in our services. This may include displaying Nokia and third party content. (Nokia Privacy Policy, our boldface)*

In this instance this could involve health data that the user may not have wanted to be used for marketing when he or she first agreed to the privacy policy. But what can you do once you have bought a product and its terms of use are amended? If you decide to stop using the product and service, it may still be too late because your personal data has already been collected. For the supplier to change the terms of use without warning is therefore a serious matter.

STORAGE

All of the apps with the exception of 2in1 include an account function which makes it possible to store information about every user of the device. The user typically has to register their email address, name and date of birth as well as various additional information concerning their health and lifestyle. The registered data is stored in the cloud, allowing the user to access the account from multiple devices. Of the apps with an account function, only Andersson and Contour allow users to use the app without creating an account, although that prevents the user from accessing their information in the cloud. It also appears that Contour's "guest function", which allows you to use the app without logging in, disappears once you create an account. 2in1 does not contain functions requiring an internet connection, which explains the absence of a user account solution.

	Andersson	QardioArm	iHealth BP7	Withings	2in1	Contour	iHealth BG5
I do not have to register an account in order to use the service.	✓	✗	✗	✗	✓	✓*	✗

* the guest function disappears when you create an account

When using cloud storage, the health data is transmitted to an external server, which means that sensitive information is moved away from the user's own equipment. As we can see, four of the seven devices do not allow users to only store data locally on their phone or another device by not creating an account. On the other hand, Andersson, Contour and 2in1 demonstrate that it is possible to deliver the service without using cloud storage. To ensure that users can retain control over the data, the Norwegian Consumer Council recommends that users always be given the option of only storing their data locally on their smartphones, unless cloud storage is absolutely necessary in order to deliver the main functions of the service.

WHICH INFORMATION IS COLLECTED – PURPOSE LIMITATION

Data mining and purpose limitation are two important privacy principles. That means that the service should collect and process as little information as possible in order to deliver the service and that the information should not be used for any other purpose than to deliver the service.[13] The more information a service collects about its users, the more vulnerable the users become. For example, data theft or leaks can result in personal information ending up in the wrong hands and being used to commit identify theft.

A balanced contract between user and service provider requires the service provider to not take unnecessary liberties with the user's information. Many free services "charge" by using collected information as a source of income, for instance. Many digital services also sell on user data as an alternative source of income, something which has created a big market for the purchase and sale of personal data.[14] If information about illnesses or other health data were to go astray, it can have unpleasant consequences for the individual in question and can result in an infringement of their privacy.

[13] Without having obtained the user's explicit consent

[14] The Norwegian Data Protection Authority has more information about how data analysis is used for profiling and other purposes. https://www.datatilsynet.no/om-personvern/rapporter-og-utredninger/temarapporter/big-data/

Many of the services ask the user to provide their full name and date of birth before they can create a user account. The Consumer Council takes the view that it is in most cases sufficient to provide an alias and possibly a year of birth in order to create a user account. We note that iHealth in particular is taking great liberties with regard to data collection. It is not content with just collecting information from its own devices:

> *Other examples of the sources we receive information include […] (b) account information, purchase or redemption information, and page view information from some merchants with which we operate co-branded business or for which we provide technical, fulfillment, advertising, or other services; (c) search term and search result information from some searches conducted through the web search features offered by our subsidiaries; (iHealth privacy policy, our boldface)*

iHealth goes on to explain that the purpose of gathering this information is marketing, amongst other things:

> *We use your collected information to improve our website content, product offerings and service specifically for you. […] 'If you do not want us to use personal information that we gather to allow third parties to personalize advertisements we display to you, please call us at 1-855-816-7705 or email to support@iHealthlabs.com. (iHealth privacy policy)*

Incidentally, none of the services reveals the extent to which they may share information or which third parties they may share information with. iHealth, Contour and MedM (Andersson) state that they may use personal data for marketing purposes, although MedM says it will only do so after specifically obtaining the user's consent.

	Andersson	QardioArm	iHealth BP7	Withings (Note: terms of use amended)	2in1	Contour	iHealth BG5
The service cannot use my personal data for marketing purposes.	✗ *	✓	✗	?	n/a	✗	✗
The service does not permit third parties to use my personal data for marketing purposes.	✓	✓	?	?	n/a	✗	?

* say that they will ask for consent

Sharing data with third parties

During the technical test, Bouvet discovered that many of the apps share user data and device data with analytics companies while they are in use. In certain cases this could be explained by the fact that certain data is required to ensure that the services run smoothly while in use. Yet such sharing can become problematic when it comes to equipment and services relating to personal health, as app usage can in itself reveal a great deal about a person's state of health.

The iOS version of iHealth Gluco-Smart makes a number of calls to multiple companies involved in targeted advertising. The app has embedded the website of the American Diabetes Association,[15] which loads automatically when the app is launched. The link to this website might seem sensible, as it provides the user with relevant information. However, the website is heavy on marketing and tracking cookies, including Krux, Doubleclick and Adfarm.[16]

The iHealth MyVitals app submits data to the Chinese company QQ,[17] known as the supplier of China's most popular chat service, amongst other things.[18] It is not clear which information is being submitted and what QQ uses it for, since the technical test could not identify the content of the encrypted data flow. However, it may be problematic that information which can potentially reveal that the user has diabetes is being transmitted to China, where privacy legislation is considerably weaker than in Europe.[19]

There may be good reasons for submitting user data to analytics companies. These third parties often supply solutions that help run and deliver the service, identify potential faults with the service and improve performance. Many of these analytics companies also sell marketing services offering user "insights". This allows service providers to "get to know their users better" by launching targeted, user-adapted advertising campaigns, for example. In the US it is common practice for pharmaceutical companies to collect "lifestyle information" from consumers in order to target their advertising, something which often leaves the user paying more.[20] Such marketing is not permitted in Norway. Similar methods are used to determine which adverts will be

---

[15] http://www.diabetes.org/

[16] *Investigation of privacy and security issues with internet connected health gadgets,* item 5.7

[17] *Investigation of privacy and security issues with internet connected health gadgets,* item 6.3

[18] https://im.qq.com/

[19] http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/583836/EPRS_ATA(2016)583836_EN.pdf

[20] https://www.democraticmedia.org/CDD-Wearable-Devices-Big-Data-Report

displayed when using services such as Facebook.[21] This sharing of information can therefore be inappropriate, especially when it is virtually impossible for the user to find out who the third parties are and how they use the information they receive.

With the exception of MedM (Andersson) all of the services allow the user to voluntarily share their readings with third parties. They can do so either by connecting the app to services such as Facebook, Twitter or Runkeeper or by directly emailing their doctor or other third parties. Although sharing health data in this way is voluntary with all of the apps, what is problematic is that they permit health data to be transmitted by ordinary email. Ordinary email is not considered secure enough to fulfil the provisions of the Data Protection Directive on information security for health data.[22]

Portability

When it comes to home testing devices, it may be useful to distinguish between the export of data to be shared with a doctor and exporting for the user's own purposes. In order to retain ownership of your personal data (such as readings), it is important that you are able to move it between different services. In an app linked to a blood pressure monitor, much of the value to the user lies in how it allows them to monitor and visualise the readings over time. If you decide to switch to a different service, it is therefore important to be able to export the readings to the new service. This will also be included as a provision in the EU's new General Data Protection Regulation, which comes into force in 2018.[23]

The Consumer Council's study found that all seven services permit the user to export their readings. The data is exported in different ways, e.g. by downloading it from the app or account page or by sending the results by email. As mentioned previously, enabling users to share health data by ordinary email may be a cause for concern. An export solution that allows users to download their readings in a universal machine-readable format directly from the service would therefore be preferable.

Of the services we examined, only Withings permits the user to import data that has been exported from other services. The other services allow the user to export data (either as an Excel file or PDF), but they do not permit data to be imported. It is therefore difficult to call it genuine portability.

[21] https://www.datatilsynet.no/om-personvern/rapporter-og-utredninger/temarapporter/personopplysninger-og-det-digitale-annonsemarkedet/
[22] https://www.datatilsynet.no/aktuelt/2016/helseapper-mangler-personverninfo/
[23] https://gdpr-info.eu/art-20-gdpr/

	Andersson	QardioArm	iHealth BP7	Withings	2in1	Contour	iHealth BG5
I can export my data.	✓	✓	✓	✓	✓	✓	✓
I can import my data.	✗	✗	✗	✓	✗	✗	✗

Deleting data

Under European privacy law, users of digital services are entitled to have their personal data deleted. Service providers are also obliged to delete personal data when storage is no longer necessary in order to fulfil the purpose for which the data was originally collected.[24] This means that all personal data relating to an individual must be deleted from the provider's servers when requested by that individual and that such data must also be deleted as soon as the purpose has been accomplished.

With the exception of Contour, all of the services examined by the Consumer Council allow the user to delete readings in the app and, with the exception of QardioArm, all of the services permit the user to delete their account on the website of the service.[25] Only Contour allows users to delete their user account in the app. Incidentally, only Andersson/MedM and Withings promise to delete all information from their servers when an account is deleted.

> *When you close your MedM account, the Service deletes all records for which you are the sole custodian. If you share custodian access for a record, you can decide whether to delete the record from the Service. (MedM privacy policy)*

It is not clear whether the other services delete all personal data from their servers or whether it is only removed from the user account and no longer visible to the user. None of the services is clear about whether they automatically delete information in the event of inactivity, for example. The only exception was Withings, which states that it will keep the data until the account is deleted.[26]

[24] Directive 95/46/EC – Data Protection Directive, article 1
[25] QardioArm's privacy policy states that the user may delete their account and information, but we were unable to establish how this is done.
[26] This pledge appears to have vanished following the switch to Nokia Health Mate

	Andersson	QardioArm	iHealth BP7	Withings	2in1	Contour	iHealth BG5
I can delete readings in the app.	✓	✓	✓	✓	✓	✗	✓
I can delete my account.	Via website	Via website	Via website	Via website	n/a	In the app	Via website

Discontinuing the service

As increasingly more objects now connect to the internet, one potentially growing problem could be that equipment will not work without an internet connection and associated app. Most people have internet access, but users may run into trouble if the app stops working for other reasons. Maintaining a digital service over time comes at a cost to the provider, e.g. the cost of running the servers. There is reason to expect this cost to cause certain digital services to be discontinued by the provider, which in turn may render physical products useless.[27]

Of the devices that the Consumer Council examined, only Andersson and Contour offer full functionality even without using the associated apps. Both devices have a digital display that lets the user view historical readings, while the apps provide added functions such as graphic illustrations. The two iHealth devices come with a basic display but no buttons, and the user can only view a reading while it is being taken. QardioArm, Withings and 2in1 do not have a display and therefore rely on the app in order to be of any use.

The suppliers of four of the apps tested by the Consumer Council reserve the right to discontinue the service at any time. This is particularly problematic in the case of QardioArm, where the physical device is rendered useless if the service is no longer being supplied. Its terms of service also suggest that it may bar users from the service without advance notice. When your data is stored on a cloud server, you will lose access to your health data if the service is discontinued. In such a scenario, there is technically speaking nothing wrong with the product (device), and that may be problematic under existing legislation.

[27] https://www.forbes.com/sites/aarontilley/2016/04/12/nests-revolv-shutdown-debacle-underscores-business-model-challenges-for-internet-of-things/#475fd54e30f5

> *We also reserve the right to suspend or end the Services at any time at our discretion and without notice. (QardioArm Terms of Service)*
>
> *We may suspend, withdraw, discontinue or change all or any part of this App without notice. (Contour EULA)*

	Andersson	QardioArm	iHealth BP7	Withings	2in1	Contour	iHealth BG5
The device can be used without an app.	✓	✗	Only single readings	✗	✗	✓	Only single readings
The service will not be discontinued without prior notice.	✗	✗	Not stated	Not stated	n/a	✗	Not stated

In the case of Withings, the company was taken over by Nokia, and users were therefore transferred to a new company which they originally had no customer relationship with. Withings Health Mate was shut down and replaced with Nokia Health Mate without giving users an opportunity to object to the transfer. An automatic update of the app, and the absence of renewed consent from the user, could lead to Nokia taking over the role of data processor on insufficient grounds. This illustrates a common problem associated with internet-connected products: services and devices may be subject to changes in functionality, and user rights may change without allowing the user to object to or cancel the service. If a user does not wish to have a customer relationship with Nokia, the only option is to stop using the blood pressure monitor. Even so, Nokia has already acquired sensitive personal data which it may go on to use for marketing purposes.