25th November 2021

Which? Response to "Consultation on the future regulation of medical devices in the United Kingdom"

Introduction

Which? welcomes the opportunity to respond to the Medicines & Healthcare products Regulatory Agency (MHRA)'s 'Consultation on the future regulation of medical devices in the United Kingdom'. Since 2020, Which? has been developing its policy and advocacy work in the area of health data, and for much longer than that Which? has tested consumer health devices as part of its Product Testing capability.

We began our policy work on Digital Health Data early 2020 in response to an explosion in popularity of consumer health and lifestyle wearables, apps and services. Now, against the backdrop of Covid-19, UK consumers are more aware than ever of the role individuals' data can play in personal and public health. Arguably, UK consumers have also become more used to using commercially available technology to monitor and manage their health and wellbeing, since the onset of the pandemic when face-to-face access to healthcare has been harder to come by for routine issues. Post pandemic, more consumers may also seek to proactively manage their health and lifestyle in order to stay well, as opposed to seeking assistance when they're unwell. We see this as a consumer driven shift from reactionary sick care to proactive health care.

The rise in the availability and affordability of digital devices has meant that there are now fitness trackers and other digital devices widely available to suit all budgets. More and more consumers are using these devices, not just as a fun way to count their daily steps, but to monitor their macros (the granular details of their food intake) or to monitor their heart health. Devices that offer such tracking of things that only a few years ago seemed like 'sci-fi' capabilities - at least on the consumer market, have also acted as a gateway to consumers who may now be buying more serious health devices for use at home.

Consumers who are used to tracking their heart rate via their watch may be more predisposed to try other devices such as blood pressure or blood glucose monitors. Indeed this may be recommended to them by health care professionals. Of course, data from such devices, apps and services needs to be analysed by medical professionals if it is to be useful in helping to identify, prevent or cure disease. At the moment, consumers only have access to one part of the puzzle, and data from consumer devices

is not generally regarded as medical grade by the medical profession. Indeed there are questions relating to accuracy of the data. This will be a critical concern should the aim for consumers to upload data from a commercial device into their patient medical record be achieved as is proposed in the Data Saves Lives Strategy[1].

Additionally, consumers are also using software to track their health and in many cases to diagnose conditions. Apps and services, some that leverage tracking from devices such as mobile phones, wearables and other connected products that gather other inputs such as mood and behaviours (to determine mental health), are effectively being downloaded and used, and in some cases informally prescribed, as medical devices.

Data is of course a key issue in this space. Data from tracking devices, apps and other services is being used to determine medical health. In some cases it is being used in an official 'medical health' capacity, in other areas it is consumer health, or lifestyle, or well being. A lack of clarity and standards around how devices and how data is classified could lead to significant consumer harm.

Our concerns therefore centre around the following key issues:

1. **What is and what isn't a medical device is unclear to consumers.**

2. **Medical devices (along with related apps and services) used for health purposes can potentially give inaccurate information to users.**

3. **How pseudo medical products are sold to consumers, and health related apps are distributed on App Stores, needs more attention.**

4. **There is potential consumer harm from using unsafe pseudo medical devices.**

5. **With smart or connected pseudo medical devices, there are not always effective protections for consumers' privacy and security.**

6. **The data protection measures must be stronger for health-relevant data.**

Our work in this space is early and is still being developed, particularly in relation to our exploration and testing of products, but our focus is on this intersection of patient medical health, consumer products and digital and data capability. Our response to the consultation is to offer our evidence from our product testing work to shine a light on some of these issues, with some commentary about our initial concerns about the space. As such, we have not therefore responded question by question.

Which? is the UK's consumer champion. As an organisation we're not for profit - a powerful force for good, here to make life simpler, fairer and safer for everyone. We're the independent consumer voice that provides impartial advice, investigates, holds businesses to account and works with policymakers

[1] UK Government, Department for Health and Social Care - Data Saves Lives Strategy, June 2021

to make change happen. We fund our work mainly through member subscriptions, we're not influenced by third parties and we buy all the products that we test.

1. What is and isn't a medical device

1.1 The scope of medical devices: the need for clarity and transparency

There has been an explosion in the popularity of consumer health and lifestyle wearables, apps and services in recent years. As many of these consumer devices replicate the functionality of medical devices, some may be classed as such. Chapter 1 of the consultation highlights the need to expand the current scope of the UK medical devices regulation. Overall Which? welcomes the expansion of the scope of the UK medical device regulations to include the additions suggested in paragraph 1.6 of the consultation, and addressed with Q78.1 and Q78.2.

There is an emergence of medical devices on the commercial market which allow consumers/users to monitor, and investigate their own physiological processes such as heart rate, blood oxygen level, temperature, electrocardiogram and even blood pressure. Consumers are using these medical products for non-medical setting purposes - i.e. for their own monitoring. This grey area of medical devices within non-medical settings poses the same risks as the original medical devices. Therefore we urge that you consider including them into the scope of UK medical device regulations, particularly as GPs are increasingly recommending such products to patients. While we do not have data about the number of apps being recommended by GPs, the fact that there is a NHS App Library also clearly indicates the NHS understands that non medical apps are being used by patients and consumers. Furthermore, the Data Saves Lives consultation outlines how data from non medical devices should be able to be leveraged alongside patient record data in a medical setting in future; indeed it is part of the strategy.

At Which?, we test several of these consumer focussed, non-medical purpose devices/features in the form of heart rate monitors or pulse oximeters as part of smartwatches and fitness trackers. Our tests raise concerns that the efficacy and accuracy of these devices may be inaccurate (see section 2), but currently they do not meet scope of the UK medical device regulations. These devices are readily available to consumers and possess the same risk as the equivalent medical device. Once again, if the intersection between consumer data and patient medical record data is to be developed, the need for accuracy from consumer facing products will be absolutely critical.

A further issue of concern to consider when expanding the scope of the UK medical device regulations is that the lines between what is a medical device is blurred when both hardware and software need to be considered. We have identified wearable devices for health and fitness that are integrating ECG monitoring capabilities as well as blood pressure monitoring. Several commercial products state that the ECG function is certified as a medical device, which is highlighted in the marketing material. However, it is not easily apparent to consumers that the software is a medical device.

For example, Samsung, Fitbit and Apple state their ECG feature is a medical device, and possess the CE mark, however, it is apparent in the terms and conditions or the small print of promotion material

that only the software/app has been certified as a medical device. Samsung states online[2] that the Samsung Galaxy Active 2 smartwatch ECG and Blood pressure apps are 'medical devices'. These manufacturers state the medical device is able to look for atrial fibrillation and clear for use with users 22 years and older. Clarification is required on the definition of medical devices and software as a medical device to ensure the consumer is informed and risks are mitigated.

With this in mind, Which? is concerned that there are commercial products such as wearables and other devices on the market that are currently not regulated by the UK medical devices regulation, yet may be used by consumers to monitor their health for discussion with medical practitioners and potentially share data with their medical records.

Which? believes there is a need for clarity for consumers - so that they understand what they are buying, what this device/service does and does not perform, how accurate the device/service is and if the device/service is providing a medical purpose. With this clarity, consumers can be clear on what they are purchasing, and be clear which products are providing accurate readings and data related to their medical health.

1.2 Intended purpose and the representation of consumer health tech as 'medical grade': the problem with wearable baby monitors

The Consultation refers to broadening UK medical device regulation to include clarifying the definition of 'intended purpose' (paragraph 1.10 - 1.13). The intended purpose of medical devices that are available to the consumer should consider manufacturer's technical documentation as well as promotional and marketing materials. These materials can promote or misrepresent the function of a medical device by association.

For example the Snuza Hero[MD] is sold as a clinically proven monitor to detect infant apnoea. The Snuza website and manuals state that it is a certified medical device and as the '*world's first portable monitor clinically proven to detect infant apnoe*a'. Whilst Snuza do not claim their product prevents sudden infant death syndrome (SIDS), testimonials (reviews) placed on their website refer to SIDS multiple times.

---

[2] Example of the term 'medical device' in the small print:
https://www.samsung.com/uk/apps/samsung-health-monitor/

Provision of CE marks for an ECG app:
https://images.samsung.com/is/content/samsung/p5/uk/apps/samsung-health-monitor/pdf/IFU_ECG_PY_20210523.pdf

Blood pressure monitor app:
https://images.samsung.com/is/content/samsung/p5/uk/apps/samsung-health-monitor/pdf/IFU_BP_PY_20210523.pdf

In addition, online material contains trusted and recommended statements; '*The Snuza Hero*^{MD} *is trusted and recommended to parents who have lost a baby to SIDS by*' and '*The Lullaby Trust - the leading charity in the UK for research and prevention of SIDS*'. Furthermore, the Snuza's online marketplace Amazon store also states its best use is for SIDs. The Lullaby Trust, a UK charity that supports bereaved families and research SIDS, has guidance on movement monitors and the prevention of SIDS. The Lullaby Trust states that '*despite the widespread use by parents there is no research evidence that monitors prevent SIDS*'[3].

We are concerned that the approach taken in the example provided may confuse consumers as to the purpose of the product, and be interpreted as a preventative measure against a highly emotive disease. It is vital that documentation; be it marketing, or advisory is accurate, and does not misrepresent the product or its function.

An additional issue is the overlap in the market with products being classed as a medical device, alongside non medical devices. Which? investigates baby products on a regular basis, covering carriers, prams, stair gates and baby monitors. We have identified a number of new wearable baby monitors that have entered the market that offer additional features - features which appear to enable the monitoring of a baby's physiological process. These include monitoring breathing, heart rate, blood oxygen level or movement. Other products that emulate the function of medical devices include:

- The Owlet (wi-fi enabled), Smart Sock Baby Monitor 3, tracks an infant's heart rate, oxygen level, and sleep trends.
- Bluebell (wi-fi enabled), Smart Baby Monitor, which monitors an infant's breathing, skin temperature and movement by a wearable device.
- Nanit (wi-fi enabled), breathing wear (swaddle, pajamas, or band), which works in conjunction with a camera to monitor a baby's breathing motion without the use of a wearable device.

Some products, such as the Owlet Smart Sock Baby Monitor 3, state the device has been '*tested to medical device standards for accuracy and are clinically validated*'. However, they are not classed as medical devices, but have the functionality of medical devices (pulse oximeter, heart rate monitor). Whilst, these products are not classed as medical devices, and therefore, not currently covered by the UK medical device regulation, the promotional material/statements may suggest a level of compliance of a product that actually falls outside the MHRA's current remit to oversee medical devices.

Which? is therefore concerned that many products in this category are currently not classed as medical devices, due to their purpose being non-medical, however, they have similar function to a medical device and potentially possess the same - and new - risks.

---

[3] https://www.lullabytrust.org.uk/wp-content/uploads/Movement-Monitors-Fact-Sheet.pdf

We are also concerned that some manufacturers are intentionally claiming their (non medical) devices offer medical benefits. They are using phrasing such as "*tested to medical device standards"* or "*clinical validated".* Such phrasing may misrepresent the products as they are not indeed regulated as medical devices. It is vitally important that these concerns are interrogated further and that the claims made by commercially available products are accurate and not misleading in any way. Once again if the intersection between consumer products and data is to blur with medical records or the seeking of medical assistance based on the reading from a commercially available product, accuracy and confirmation that the product is of medical device standard and clinically accurate is vital.

2. The efficacy of pseudo medical devices and apps

Which? has a strong product testing capability which powers our product reviews, enjoyed by our members via online services and our magazines. We rigorously test a range of devices, including in the consumer health space, such as thermometers, pulse oximeters, smartwatches and fitness trackers. The following evidence is provided to highlight issues we feel are important when considering the regulation of medical devices in particular the pseudo medical devices that we have identified which have notable efficacy issues that should be considered by the regulator.

2.1 The efficacy of wearable consumer health tech: widespread inaccuracy

Increasingly in the consumer health space, we've seen an emergence of devices that don't claim to be 'medical' devices, but offer a health-relevant function to consumers. This primarily includes smartwatches and fitness trackers, which we test on a monthly basis. We have found an increased amount of technology that monitors physiology. Wearable technology allows consumers to monitor, investigate and track their own physiological processes.

Which? has found over the course of 2019, that 97% of the 109 models tested possess an integrated optical heart rate monitor, allowing consumers to monitor heart rate in real time. Currently, Which? actively tests the accuracy and reliability of the integrated heart rate monitor of these devices. We have found that some of these models can be inaccurate and unreliable.

Less than half of models tested (49%) exhibit a high level of accuracy when compared to a reference device (percentage difference of less than 5%). During different exercises (walking, running and cycling), the level of accuracy differed considerably, with only 29% of models performing with an error of less than 5% during walking. 48% of models had an error of less than 5% when testing while participants were running. The accuracy improved when participants used an exercise bike, with 80% of tested models having an error of less than 5%.

Additionally, we have identified that 49% of the 109 models possess pulse oximeter functions similar to that of a photoplethysmogram, allowing consumers to measure blood oxygen saturation (SpO2). We have so far tested 20 models for the accuracy of the pulse oximeter features in smartwatches and fitness trackers. We found issues with 4 devices that could not detect SpO2 values on individuals with

dark skin tones. Furthermore, we found that 13 devices exhibited highly variable results when tested on different panel members, with a root mean square error (Arms) greater than 4%[4]. Particular requirements for basic safety and essential performance of pulse oximeter equipment, the accuracy of pulse oximeter shall be a root-mean-square difference of less than or equal to 4.0 % SpO2.

In addition to these features, Which? has identified the integration of other features with similar functions to medical devices. Which? has found nine models from Samsung, Apple and Fitbit that possess the capability of performing an electrocardiogram (ECG). We have also identified five models from Fitbit, Huawei and Mobvoi that possess skin temperature sensors allowing consumers to monitor their temperature. Furthermore, we have found six devices with the capability of measuring blood pressure.

Whilst the heart rate monitor on smartwatches and fitness trackers are not classified as medical devices, they do monitor physiological processes, and can exhibit high levels of variability. Whilst the pulse oximetry function on smartwatches and fitness trackers are not classified as medical devices, they can also exhibit high levels of variability. Both these types of devices are therefore posing the same risk as the corresponding (and regulated) medical devices if not used responsibly by consumers (see Section 4).

Manufacturers do not claim these products are medical devices, or have the intended purpose to 'diagnose, prevent, monitor, treat, or alleviate disease'. However, certain health tech features being integrated into Smartwatches and fitness trackers do investigate/monitor physiological processes, meeting the requirement iii. of the medical device definition. Specific features such as ECG technology is being certified whilst the remaining technology (heart rate monitor, pulse oximeter) is not certified. With consumers using these devices and their features to monitor their health and wellbeing, the line between medical device and non-medical device is so intensely blurred to become potentially problematic.

3. The sale of medical devices by distance sales: the need for regulation

The consultation highlights that the UK medical device regulations do not include requirements for distance sales of medical devices (section 9 - Distance sales). Medical devices are available to consumers by distance sales; they can be bought from high street retailers as well as online marketplaces such as Amazon, Ebay, and Wish. We have investigated products available from online marketplaces and have identified safety issues. We have concerns that unsafe products can be removed from online marketplaces, but can reappear at a later date or on another platform. This issue can affect medical devices available via distance sales.

[4] According to the BS standard BS EN ISO 80601-2-61:2019

We are currently investigating the accuracy and legitimacy of medical devices such as digital thermometers and pulse oximeters, purchased from online marketplaces. We wish to inform consumers of the risks of purchasing 'cheap' healthcare products from these marketplaces. As part of this we are examining the medical device certification to ensure the CE mark complies with the Medical Devices Regulations and meet the performance requirements stated in the standards. We will have more evidence to share on this in due course.

Which? welcomes and supports the intention of the MHRA to amend the UK medical device regulations to clarify that a medical device, or any diagnostic or therapeutic service involving a medical device, sold or supplied (even for free of charge) via distance or electronic means, for example via a website or app store, must comply with the UK medical device regulations. We also support the intention to amend the regulation to require individuals, company or organisation offering a medical device by distance sales to provide a declaration of conformity.

4. There is potential consumer harm from unsafe pseudo medical devices

There are, of course, benefits from consumers using pseudo medical devices to monitor and improve their health. This can reduce the burden on NHS services and also increase the armoury of preventive measures for a range of conditions that may emerge. However, there is also a clear danger with devices that purport to deliver a monitoring, tracking or even diagnostic function, particularly if there is even a hint that this could prevent a highly emotive condition (such as infant SIDS), yet there is no clear clinical evidence to prove such efficacy.

As we have detailed earlier in this report, pseudo medical devices can have variable levels of accuracy, and this could lead to someone making an incorrect assumption about their health status - either worrying too much and contacting medical services for no reason, or by contrast worrying too little and having a false sense of security.

For example, the Lullaby Trust issued a report[5] on baby movement monitoring products, and while it noted that there can be some benefits from the technology, it also stated that:

"Parents may rely upon the monitor for assurance that the baby is well and may not look out for other signs of illness or observe the baby's overall health and development".

In addition, we have seen evidence that these devices, particularly those with sensor technology, can function differently depending on the use (eg, sensor technology on different skin tones). This can lead to potentially variable outcomes - we note that the MHRA itself has issued its own warning[6] over

[5] Lullaby Trust, Movement Monitors CONI Coordinator information

[6] BBC News 31st July Covid: Pulse oxygen monitors work less well on darker skin, experts say

use of pulse oximeters by patients from black, Asian and other ethnic minority groups without engaging medical advice first and that concern around racial bias in the use of oximeters has now led to a review being called by the Secretary of State for Health[7].

We are also concerned over the potential for monitoring technology to actually increase anxiety in the user. We hear anecdotal reports of users of fitness trackers stating an increased sense of anxiety over not doing enough activity to ever satisfy the health programme. There are also dangers with inaccurate readings giving 'false alarms' that can raise anxiety. As the Lullaby Trust indicates:

"Movement monitors can give false alarms which may heighten a parent's anxiety and lead to disturbance of the baby's sleep. False alarms may occur for a variety of reasons - the sensor pad becomes detached, or the abdominal movements become so slight that they are not detected."

Inaccurate health monitoring equipment can potentially lead to bad health outcomes, with either the user being overly cautious or too dismissive of true health indicators. Health monitor kit could potentially increase health anxiety, particularly if it gives false alarms over sensitive conditions.

5. The security of medical devices: Avoiding the 'regulatory gap'

The consultation raises concerns over the requirement for cybersecurity and information security for medical devices, in particular software as a medical device (section 64). An increasing number of pseudo medical devices now have smart, or connected functionality, meaning they can directly connect to the internet, or use an additional device, such as a smartphone, to do so. This opens up a range of more advanced functionality powered by online servers. We have seen a wide variety of smart health products, including pulse oximeters, blood pressure monitors, blood glucose monitors, baby movement monitors and even a smart nicotine dispenser. We have also tested smartwatches and fitness trackers for many years.

Alongside the inaccurate data readings and blurred lines between medical and non-medical software functions, there is an additional layer of consumer detriment here in their security against malicious hackers, and the protection of their data privacy.

5.1 Security

Over the last eight years Which? has been working to highlight the widespread problems of connected devices not having proper security safeguards against malicious hackers. This can lead to consumer's data being stolen, their devices being tampered with or other valuable devices they own

[7] BBC News 22nd November 2021 Covid: Sajid Javid orders review of medical device racial bias

being targeted. Hacking attacks can also lead to surveillance and privacy intrusions, and we are just beginning to understand the levels of detriment associated with that (eg, uses of stalkerware in domestic abuse cases).

Although standards have improved in a number of areas, such as wearables, we are concerned that health related smart devices may have poor security practices that could potentially be harmful to consumers.

As a consumer charity, our primary focus is on devices that consumers can purchase directly, so we have not reviewed the requirements for currently on-scope medical devices as cited in Q64.1. However, we have widely reported on there being no baseline of regulation for consumer products on sale in the UK, yet consumers believe that if a device is on sale, then it is secure.

We welcome the introduction of the Product Security and Telecommunications Infrastructure (PSTI) Bill[8], which will inject a baseline of security to devices and also amplify use of the EN 303 645 technical standard for security that was introduced in 2020. However, we know that this baseline will not go far enough to deal with all the problems of insecure products, and more must be done. Equally, we acknowledge that the PSTI Bill will not cover medical devices, but are concerned that this will lead to a 'grey area' of regulation for devices such as smart pulse oximeter and blood pressure tech, in which the new product security regulator and the MHRA could become unclear on where each's regulation duty begins and ends.

Finally, we have expressed concern in the past over clone, fake or derivative products that flood online marketplaces and are effective copies of popular devices. These products often ape a popular product, such as an Apple Watch, and appeal to consumers because they are much cheaper than the original version. We conducted a search on 24 November 2021 for 'smart watch' on eBay and found 43,352 models[9] listed as 'unbranded'.

So, any effort to introduce greater security standards on smart health devices must also look to tackle the 'shadow' market of fake and clone products that abounds via online marketplaces. More on this can be found in a recent report[10] we published showing more than 1,800 devices being sold with security and privacy risks. Most of these are clones.

The market for smart health and medical devices is booming, and leads to a shadow market of clone and derivative technology sold via online marketplaces. There are no baseline regulations for security standards currently, although this will come when the PSTI Bill comes into force. The PSTI Bill will

---

[8] UK Government, Department for Digital, Culture, Media and Sport, Product Security and Telecommunications Infrastructure Bill

[9] Ebay smart watches

[10] Which? Hack Friday: Online marketplaces flooded with insecure smart products, 16th November 2021

exclude medical devices, but could lead to a regulatory gap with smart health devices and associated technology.

6. Greater scrutiny of data collection and data security needed in commercial health products.

While the security risks covered above are pressing concerns, there is also an ongoing and harder to tackle risk to consumer's privacy from using smart devices. The UK's data protection regime under the UK GDPR has increased standards in some ways e.g. with privacy policies and data tracking measures. Additionally there have been efforts by App Stores to make app downloads more transparent with aspects such as data permissions. However, in our experience it remains a challenge for consumers to fully understand what they are signing up to when they use health devices and apps.

For example, we recently investigated a smart product app (which we cannot name as talks with the company are ongoing) that acts as a platform for more than 4,000 different device types that consumers can buy, mostly home sensor technologies. Despite utilising two highly trained lawyers, it was hard to fully understand what data sharing agreement the user was entering into when they signed up to the app. This is a common issue and it often results in consumers simply surrendering to 'click accept' just to use the device or app that they want to use.

We are also concerned about the use of cookies and other marketing trackers when consumers engage with health tech products and services. In June 2021, we reported that when you click on the website for WW (formerly Weight Watchers), there are 225 cookies in use, including 87 there to track the user. As you can see in Figure 1, many of the cookies were being operated by third-party advertising firms, including YouTube, Google, Yahoo and AppNexus. One of the highest cookies pages on the site (with more than 100 active) was the main page of the privacy policy.

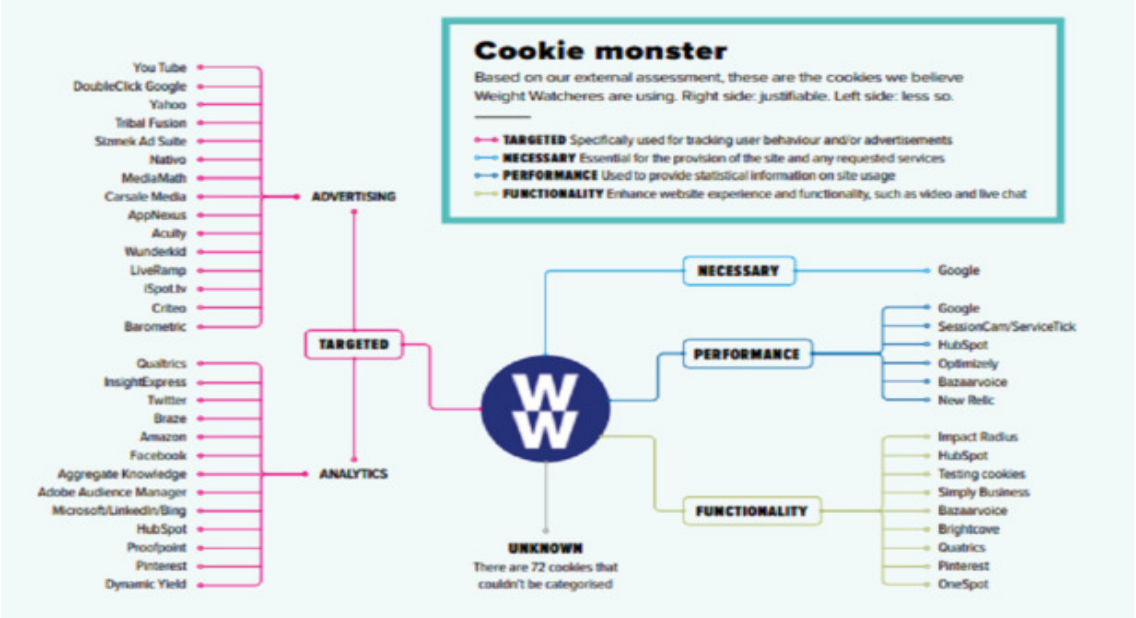

Figure 1: Fit for Purpose?: The health apps that pose security risks, Which?, June 2021[11]

In addition to apps that are designed for use with a specific device, Which? also assesses apps that are designed for use with a smartphone or tablet, so this device then becomes by extension the smart health product (including potential use of biometric and tracking sensors). We have found issues with these apps, too. We published a report in 2021 covering the widespread privacy risks of health related apps and services. This exposed a range of risks with general health apps[12], medical apps[13] and baby apps[14].

Not only are issues such as overzealous use of cookies, vague privacy policies and excessive use of trackers at play with these apps, but also there can be issues with poor security practices being put in place that could put consumer data at risk (see above example of The Wonder Weeks baby app). Poor data security and a failure to adequately or meaningfully adhere to data protection law can put the sensitive personal data of consumers at risk of misuse or abuse.

[11] https://www.which.co.uk/news/2021/06/fit-for-purpose-the-health-apps-that-pose-security-risks/

[12] Which? News ' Fit for purpose?: The health apps that pose security risks', 9th June 2021

[13] Which? News 'Ada, Babylon and WebMD: can you trust medical apps with your health?' 9th June 2021

[14] Which? News 'Popular baby monitor app put privacy at risk' 9th June 2021

Summary

In summary, having carried out extensive product testing and begun in-depth policy investigations in this space, Which? has several broad ranging concerns about the regulation of medical devices and the broader consumer health ecosystem. We support many of the amendments proposed by the consultation and have wider suggestions that we would encourage the MHRA to consider.

1. Provide clarity of scope of general medical devices

Overall Which? welcomes the expansion of the scope of the UK medical device regulations to include the additions proposed in paragraph 1.6 of the consultation. However, clarity must now be given to the wider health market where there is any process that could lead to medical outcomes. We would therefore welcome clarity on what is and what isn't classed as medical devices - especially in the apps, wearables and mobile phones space.

If there are commercially available products such as apps, wearables, mobile telephones that include points 1.9a - 1.9d then it must be made clear to consumers that they are classed as medical devices. In addition, these devices must have a greater level of scrutiny to them applied before they reach the market.

Overall, it could be beneficial to expand the scope of the UK medical devices regulations to include some of the examples given in evidence above and place these features and functions under a greater level of scrutiny.

2. More clearly define Software as a Medical Device

Since software used as a medical device in these health care products is heavily reliant on data generated by the integrated hardware (sensors), we would urge you to clarify the definitions of *Software as a Medical Device,* and define the framework in which *Software as a Medical Device* differs from the hardware. Clarity is required for consumers since wearable technology is integrating medical device functions to monitor physiological features, and acquiring medical device classification, however, this is restricted to *Software as a Medical Device* and not to the entire device or its other medical device functions

3. Require transparency around intended purpose

Which? welcomes the change to make clear that 'intended purpose' should be construed objectively and that key materials such as a manufacturer's technical documentation may be used as evidence of intended purpose. Additionally, marketing material should also be considered as evidence for intended use.

4. Require regulation of devices sold via distance sales

Which? welcomes the intention to amend the current UK medical devices regulation on the distance sales of medical devices, or any diagnostic or therapeutic service involving a medical device to ensure that compliance with UK medical device regulation is complied with. We also support the intention to amend the regulation to require individuals, company or organisation offering a medical device by distance sales to provide a declaration of conformity.

5. Introduce mandatory compliance with 'ETSI EN 303 645: The European Standard on connected device security' for pseudo medical devices with a smart or connected extensions

Which? welcomes efforts to increase security of connected/smart products that impact consumers, either directly or indirectly.

Which? has been doing extensive work with the Department of Culture, Media and Sport on the Product Security and Telecommunications Bill that is now making its way through Parliament. While Which? is broadly supportive of this legislative effort to improve standards, we are also concerned about some categories of smart products falling into a 'regulatory gap', and believes this could include smart pseudo medical products.

By regulatory gap we mean that products such as smart pulse oximeters or smart blood pressure monitors could be wrongly assumed as being covered as medical devices and therefore no security scrutiny applied to them. Equally, as these devices handle sensitive medical data in some instances, the need for high levels of security is even more paramount.

Which? therefore proposes that any devices designated as smart medical devices should comply with the ETSI EN 303 645 technical standard before they can be listed for sale. A similar approach has already been proposed in a number of other potential 'gap' areas, including smart toys, electric vehicle chargers and Customer Premise Equipment (CPE) routers. We feel that it will have a similar value in the smart medical device market in raising standards.

6. Review of data privacy requirements in pseudo medical devices needed

In light of our work exposing poor data privacy and security in a range of commercially available apps defined as health apps, we would urge a review of the privacy protection guidelines for apps (both smart health device extension and standalone apps) that are available to UK consumers. We note that there are some existing 2013 Ofcom/ICO guidelines for this[15]. However, we feel that these need to be updated and that health apps should be treated as a special case as with smart product security listed above.

[15] ICO Privacy in mobile apps. Guidance for app developers

For further information about Which's work please contact:

Product Testing: Andrew Laughlin andrew.laughlin@which.co.uk

Policy: Renate Samson renate.samson@which.co.uk