HACKERS, BREACHES AND THE VALUE OF HEALTH DATA

THE ULTIMATE GUIDE TO PRIVACY IN DIGITAL HEALTH

Dr. Bertalan Meskó
The Medical Futurist

Hackers, Breaches and the Value of Health Data

The Ultimate Guide To Privacy

In Digital Health

Dr. Bertalan Meskó
The Medical Futurist,

Dr. Pranavsingh Dhunnoo,

Judit Kuszkó

Andrea Koncz

TMF+
THE MEDICAL FUTURIST

Table
of Contents

Welcome message from The Medical Futurist

Dear Reader,

Through the content produced by The Medical Futurist Team and the research made by The Medical Futurist Institute, we have been discussing the context and the future of digital health for almost two decades. We have addressed how advanced technologies can make patients the point-of-cares and how the use of those can lead to a better doctor-patient relationship.

We are obviously on the techno-optimistic side of the ongoing debate about how digital health will shape the future of care. However, we also always emphasise that digital health is a cultural transformation that impacts the traditional structure of healthcare.

By 2022, it has become clear that this is the way forward: using advanced technologies while keeping the core values of medicine in the spotlight: empathy, attention and time. Governments have published digital health policies; medical associations have started to lead this movement and empowered patients worldwide have begun to make their physicians empowered too.

Far the biggest obstacle in this long process is the issue of privacy. Simply put, there is no digital health without sacrificing a part of our privacy. Without data, without our data, advanced technologies cannot improve and there is no way we can implement them in the everyday practice of medicine.

The real question is not whether we should do this, but how we can do it in a way that we protect what is valuable and vulnerable. How do we use artificial intelligence, health sensors, personal genomics or portable diagnostic devices to support medical decision making while not hindering the sacred private pieces of information of patients.

Welcome message from The Medical Futurist

This is what this executive summary describes in detail. We aimed at creating a guide that 1) gives a clear picture of what might happen to our data in the digital health era, while 2) also providing recommendations about what average users can do to protect what is important to them. And have no doubts, we are all users of these technologies whether we decide to participate or not.

At The Medical Futurist, we firmly believe that patients or users of these technologies must be in a position where they can decide how much of their privacy they are willing to give up or share in exchange for a chance for a longer and healthier life. This is the social contract we need to keep a close eye on. And that's what we hope we can help you with through this e-book.

Please feel free to share your questions, doubts and fears about privacy around digital health because that is the only way we can find common ground with technology companies, providers and governments.

The wide and successful adoption of digital health technologies can only take place if we can efficiently deal with all the privacy issues and educate the general public about the threats they have to know about.

It is for the sake of patients and their safety.

I hope you will find our publication a useful weapon in this battle.

Kind regards,

Dr. Bertalan Meskó,
Director of The Medical Futurist Institute
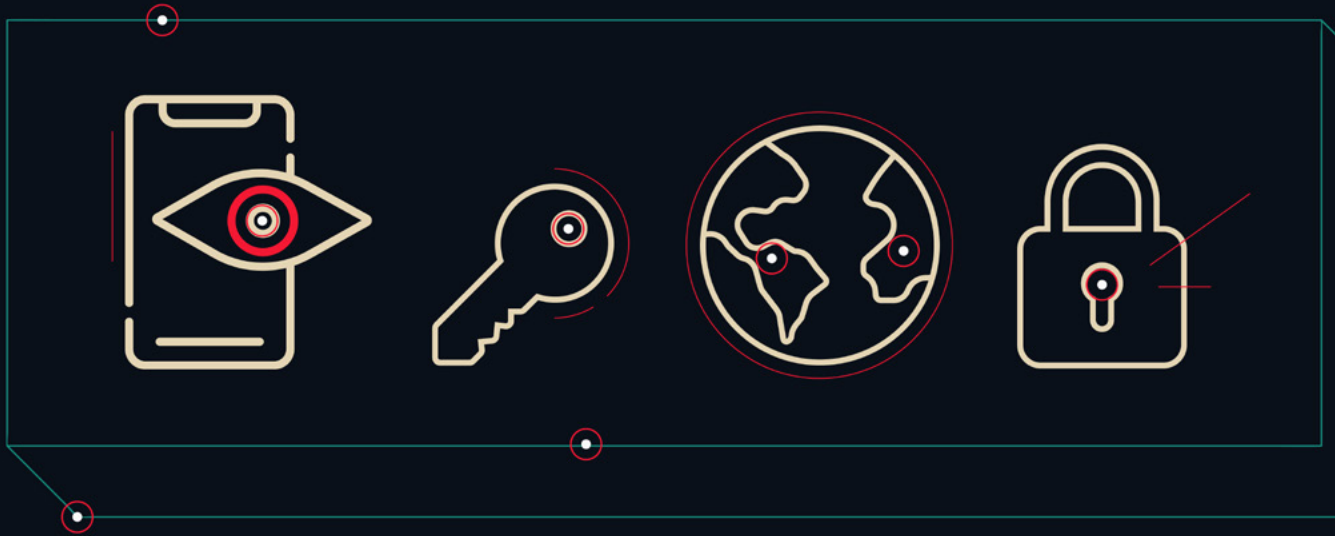
Introduction
The need to upgrade privacy protection in the digital health era

Traditionally, [health data would be described as](#) any information "related to health conditions, reproductive outcomes, causes of death, and quality of life" for an individual or population. This definition might be due for an update. Nowadays, health data is not only generated in the traditional way but also by healthcare IT systems and novel technologies constantly amassing vital metrics inside and outside of healthcare institutions. The amount of health data on every single individual is increasing at an unprecedented rate and is bringing along a new dimension to security, privacy, and ethical concerns.

Healthcare institutions and regulatory authorities must deal with this load of information like never before. Are they prepared to do so securely? Such sensitive information is already among the most valuable on the black market. The value it holds for fraudsters to make false insurance claims and buy medical goods illegally is leading to increased compromised healthcare records. In the first half of 2021 alone, that amounted to [almost 45 million potential breaches](#) in patient records.

The security and privacy protection of this sensitive health information rely on healthcare authorities, but in the digital health age, they might not have an oversight of the whole landscape. Unfortunately, patients, or the actual source of these data, are traditionally hin-

dered from accessing their information. But patients must be part of the privacy discussion and demand secured measures over the handling of their data.

In the five introductory sections below, we discuss the themes that lead to a demand of upgraded privacy protection in the digital health era. We then follow up with the corner-stones of privacy discussion in this era, which are expanded upon in the whole e-book.

There are five major reasons why we have to tackle the privacy issue now and how we got to a point where further developments in healthcare are impossible without solving the privacy puzzles first.

The source of my health data

Data in the cloud

EEG

Smartphone

Smartwatch ECG

Fitness Tracker

Blood test

Medical Records

Microbiome

Medications

DNA data
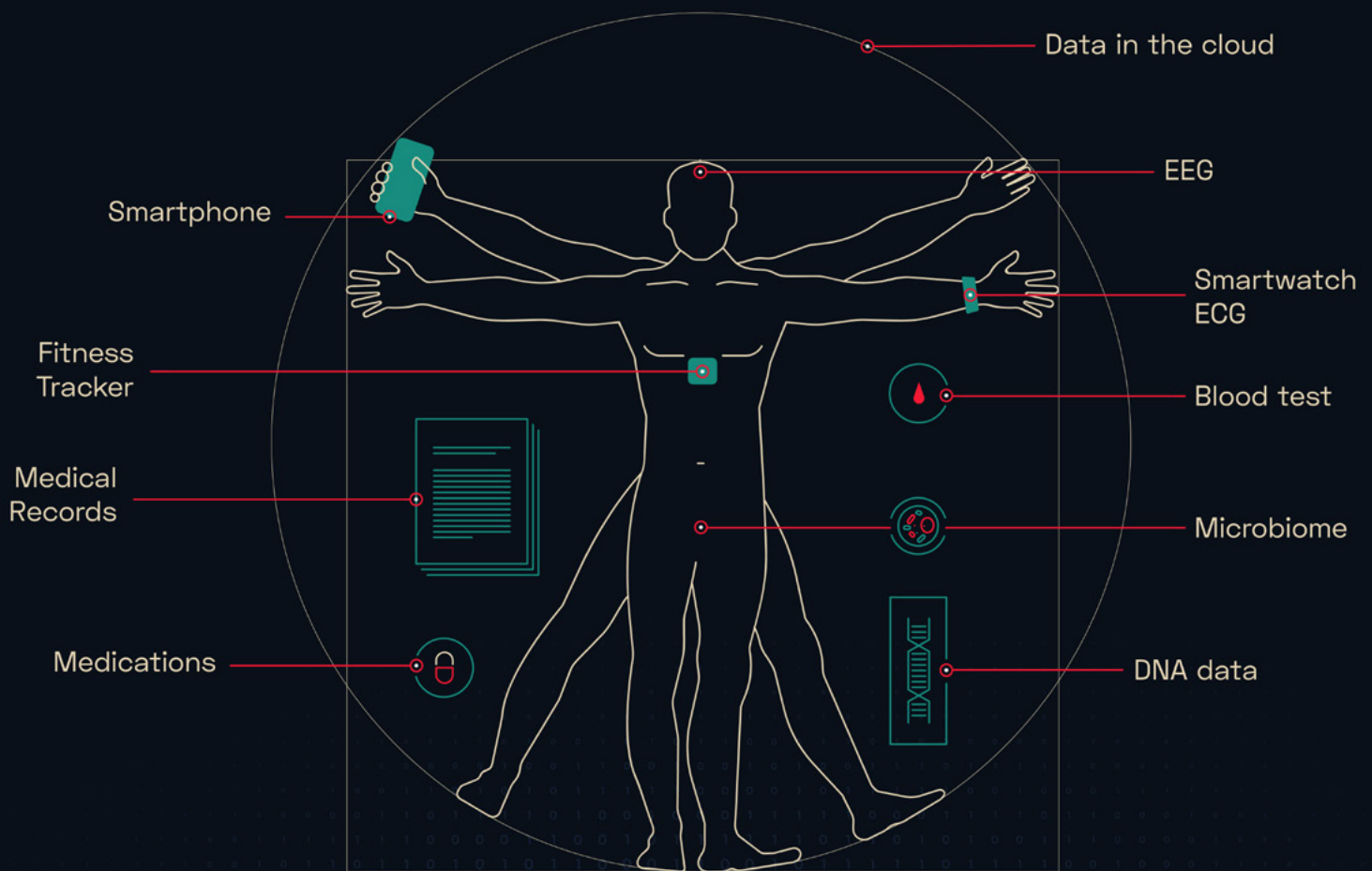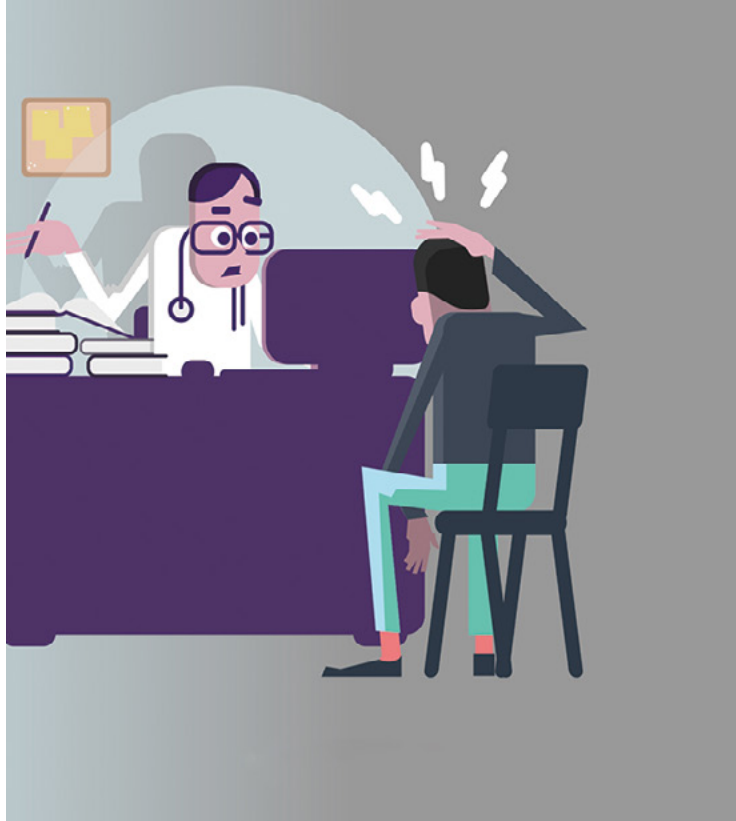
The rise of advanced technologies and of the empowered patient

Digital health is going to replace traditional technologies as we know it. It will upend the traditional, hierarchical model of healthcare where patients are neither empowered in their care nor treated as equal-level partners. We already see it reap its fruits because we already are in the digital health era. Along with this era comes the rise of the empowered patient and new issues around privacy and security. But before diving into these, it might help to go down the memory lane and visualise what brought digital health along.

For long, healthcare matters were relegated to the ivory towers of medicine with medical professionals as the immovable gatekeepers. They were better suited to deal with patients' ailments and the information that they generate. However, this paternalistic doctor-patient relationship began to change with the prevalence of chronic conditions. Management of the latter can span decades, and its success relies on a more cooperative approach between doctors and patients. This partnership-like approach also evolved with the increasing importance of the bioethical principle of informed consent, where the need for such a relationship is stressed.

It goes without saying that technological developments also weighed heavily to usher this era. But this too was a stepwise influence. The widespread adoption of personal computers in the 1990s led to the emergence of e-health. This was followed by telemedicine with the advent of the internet. In the early 2000s, social media paved the way for medicine 2.0 and health 2.0, while smartphones led to mobile health.

The exponential rate of disruptive technologies breaking into healthcare in the 2010s really led to a boom in digital health. With accessible digital health tools such as online communities, smart sensors and mobile apps, access to healthcare is available outside its ivory tower bubble. The E-patient demands better access to their health data so that they can better manage it along with healthcare professionals. This rise in healthcare Big Data is, however, also attracting other players outside the doctor-patient relationship.

Health data is the new oil

With the undeniable advantages that digital health brings along, we also face an unprecedented challenge. We have to ensure the security and privacy of the load of patient data that comes with the increased use of these technologies. This unprecedented access to such information essentially makes health data the new oil.

This analogy has been gaining traction lately, and it's not without good reasons. Like oil, the value of health data depends on how refined that commodity is. The more refined it is, the higher price it will fetch. Recent estimates put the value of electronic health record (EHR) data aloneat around at around £100 per record. However, combining EHR data with genomic and phenotypic data raises the value to £1000–5000 per record. The NHS, or the largest integrated health care provider in the world, holds on to 55 million patient records with a curated dataset valued at around £5 billion per annum.

In fact, health data might be even more valuable than oil since its value does neither depreciate with use nor is it a finite resource. Institutions can use and reuse the data collected; and in the digital health age, new medical data is constantly being generated. This ability of health information to be reused can have different implications in the long term compared to why we gave it away in the first place. For instance, in the U.K., patient data from the NHS was used to trace and potentially arrest people who lacked proper authorisation to stay in the country. The information was likely given to receive medical care and the source of that information, the patient, had no idea that it could be used against them.

Not only healthcare institutions hold on to these data but also social media companies, websites and wearables that the average user employs for their wellbeing. Private companies are harvesting this newfound treasure trove of health information and exchanging it for revenues and profits. In fact, stakeholders across the healthcare landscape from pharma companies through startups to governments want to monetise patients' data, and they are often in cahoots with each other. Let's consider the health information sharing website Patientslikeme. It helps patients share detailed information about their ailments so that others can get to know what works and what doesn't for a specific case. But Patientslikeme is also monetising such information by selling anonymised patient data to its partner pharma and medtech companies.

Patienslikeme is only one of the growing examples of seemingly-helpful services monetising over intimate data. In the digital health era, it's easy to get lost and not to know where to look as our sensitive data is getting stored and used everywhere and even being profited on without our knowledge.

The privacy discussion and cultural transformation needed for the digital health era

As we've highlighted, health data is turning into an increasingly valuable and coveted commodity; so much so that companies that traditionally have nothing to do with healthcare are going after such information. This is especially the case in the online advertising revenue industry and the age of social media; and you might already have signed a pact with the devil without even realising it.

For instance, by following internet users' online habits, Facebook allowed targeted pharmaceutical ads for years. This is becoming a growing concern as even users who don't explicitly reveal whether they need or are following a treatment are receiving such ads. To improve their services, such Big Tech companies are further employing unscrupulous techniques such as listening to voice conversations. Facebook, Amazon, Google and Apple have all been found to listen to conversations of users of their services. Since they went public, these companies paused such practices or offered opt-out features from having their audio recordings sent for human review.

Despite setbacks, private companies aren't letting go of the potential of the data market. All of these Tech Giants listed here and more are marching steadily towards the healthcare landscape.

A legendary example was how Britain's NHS shared 1.6 million patients' health data with Google's DeepMind. The information included data from the last five years, complete with critical care, and emergency department records, day-to-day hospital activities, and results of pathology and radiology tests, while patients were left in the dark if and how they can opt-out.

They are adopting a consumer-centric approach and even offer personalised insights into the patients' own health with the help of digital technologies. But it's not without its issues.