# Do you think data theft couldn’t be an issue for you? Think again!

Petra Wildemann
10.5.2018

When we hear about stolen personal data and read reports, many of us tend to think that this has little or nothing to do with us. This kind of thinking could not be more mistaken!

Sensitive personal data in the healthcare business is a topic we tend not to think too much about. But data in the healthcare business is a lucrative target for hackers. As the healthcare industry often has to very quickly process sensitive patient/customer data, their websites are often exposed to hackers and their storage drives are often unencrypted.

We don’t always make the connection between the use of modern technology and the practice of data collection. As an example, we drive cars that remember our driving behaviour. When a car is taken in for service, the mechanics download the data. This is a great way to identify potential damage and risks for the car and the driver. On the other hand, this is also private data, recording driver behaviour for the past weeks or months, whenever the car was used.

Another data collection device we tend not to pay attention to is hearing aids. Though we tend to associate these devices mostly with the elderly, they are increasingly also used by younger people who have damaged their hearing, for example through overuse/abuse of headphones or earphones.

It is becoming increasingly commonplace for hearing aids to have the capacity to monitor vital signs for the purpose of measuring eg blood pressure, heart rate, body temperature, pulse oximetry and ECG. This capacity has obvious health benefits, but it also means that sensitive data is reported to doctors and others in the healthcare industry. There is evidence that such data can be attractive for hackers.

Hearing aids also sometimes direct people through traffic, in train stations, across the street, etc. This also creates dangerous potential, as hackers can direct use this technology to direct people to places where they do not want to go for reasons which are decidedly not in their interest.

Another example: smart watches, which can collect fitness and other health data.

There are many challenges ahead of us with respect to this topic. We need to increase our awareness of the range of data that is at risk, and of the potential for misuse of this data.

It will be interesting to see what effects the new GDPR regulations have in this area.