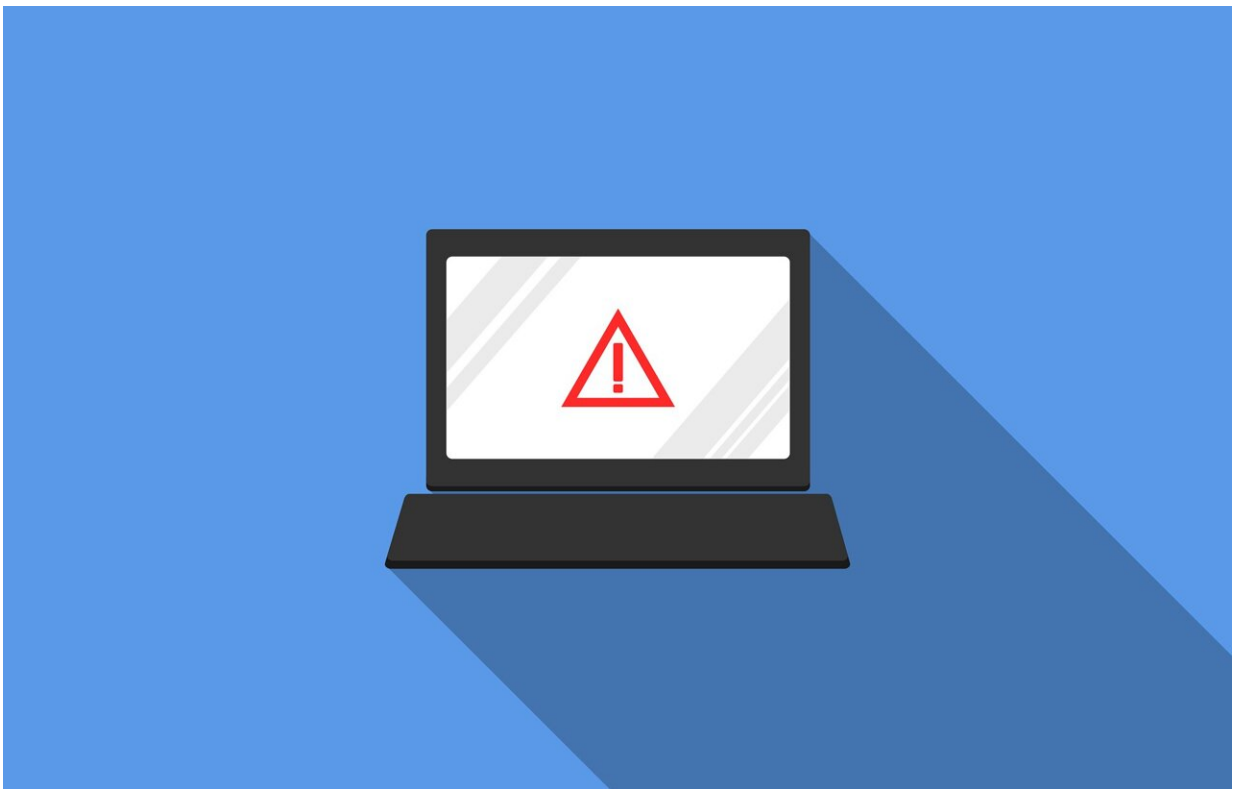# Attempts to access Kate Middleton's medical records are no surprise. Such breaches are all too common

March 21 2024, by Bruce Baer Arnold

Credit: Pixabay/CC0 Public Domain

The [alleged](#) data breach involving Catherine, Princess of Wales tells us something about health privacy. If hospital staff can apparently access a future queen's medical records without authorization, it can happen to you.

Indeed it may have already happened to you, given many breaches of health data go under the radar.

Here's why breaches of health data keep on happening.

What did we learn this week?

Details of the alleged data breaches, by [up to three staff](#) at The London Clinic, emerged in the UK media this week. These breaches are alleged to have occurred after the princess had abdominal surgery at the private hospital earlier this year.

The UK Information Commissioner's Office [is investigating](#). Its report should provide some clarity about what medical data was improperly accessed, in what form and by whom. But it is unlikely to identify whether this data was given to a third party, such as a media organization.

Health data isn't always as secure as we'd hope

Medical records are inherently sensitive, providing insights about individuals and often about biological relatives.

In an ideal world, only the "right people" would have access to these records. These are people who "need to know" that information and are

aware of the responsibility of accessing it.

Best practice digital health systems typically try to restrict overall access to databases through hack-resistant firewalls. They also try to limit access to specific types of data through grades of access.

This means a hospital accountant, nurse or cleaner does not get to see everything. Such systems also incorporate blocks or alarms where there is potential abuse, such as unauthorized copying.

But in practice each health records ecosystem—in GP and specialist suites, pathology labs, research labs, hospitals—is less robust, often with fewer safeguards and weaker supervision.

This has happened before

Large health-care providers and insurers, including major hospitals or chains of hospitals, have a worrying history of digital breaches.

Those breaches include hackers accessing the records of millions of people. The Medibank data breach involved more than ten million people. The Anthem data breach in the United States involved more than 78 million people.

Hospitals and clinics have also had breaches specific to a particular individual. Many of those breaches involved unauthorized sighting (and often copying) of hardcopy or digital files, for example by nurses, clinicians and administrative staff.

For instance, this has happened to public figures such as singer Britney Spears, actor George Clooney and former United Kingdom prime minister Gordon Brown.

Indeed, the Princess of Wales has had her medical privacy breached before, in 2012, while in hospital pregnant with her first child. This was no high-tech hacking of health data.

Hoax callers from an Australian radio station tricked [hospital staff](#) into divulging details over the phone of the then Duchess of Cambridge's health care.

Tip of the iceberg

Some unauthorized access to medical information goes undetected or is indeed undetectable unless there is an employment dispute or media involvement. Some is identified by colleagues.

Records about your health *might* have been improperly sighted by someone in the health system. But you are rarely in a position to evaluate the data management of a clinic, hospital, health department or pathology lab.

So we have to trust people do the right thing.

How could we improve things?

Health professions have long emphasized the need to protect these records. For instance, medical ethics bodies [condemn](#) medical students who [share](#) intimate or otherwise inappropriate images of patients.

Different countries have various approaches to protecting who has access to [medical records](#) and under what circumstances.

In Australia, for instance, we have a mix of complex and inconsistent laws that vary across jurisdictions, some covering privacy in general,

others specific to health data. There isn't one comprehensive law and set of standards vigorously administered by one well-resourced watchdog.

In Australia, it's mandatory to report [data breaches](#), including breaches of health data. This reporting system is currently being updated. But this won't necessarily prevent data breaches.

Instead, we need to incentivize Australian organizations to improve how they handle sensitive health data.

The best policy [nudges](#) involve increasing penalties for breaches. This is so organizations act as responsible custodians rather than negligent owners of health data.

We also need to step-up enforcement of data breaches and make it easier for victims to sue for breaches of privacy—princesses and tradies alike.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation