The future is digital – but is it safe?

Joined-up patient-centred care requires sharing of data between patients, oncologists, hospitals, labs, GPs, nurses and even social care. But as apps designed to gather and share this data proliferate, so does the risk that the data ends up in the wrong hands, and possibly in identifiable form, as **Peter McIntyre** reports.

Following treatment for prostate cancer in 2015, Eric Hounslow from Hampshire in England joined a "supported self-management" study at University Hospital Southampton for follow-up care.

It was his second cancer. Six years earlier he had undergone surgery for an unrelated kidney cancer and experienced a traditional follow up of regular tests and anxious waits for results. Today there is virtually no waiting. He uses the internet to access the results of PSA tests almost as soon as they are done.

"It's an extremely tense time, because so much rests on what they're going to tell you," he says. You're praying for good news, but waiting a week or more to find out. Now I can give my blood at 9.00am and access the results myself later that day, saving me from all that stress every six months.

"I can access my appointments, medical details, personal information and surgery reports from anywhere in the world. I can also communicate with my surgical team quickly and easily. As someone who has experienced both systems, I'd recommend this scheme to anyone."

Eric Hounslow, now 72, is just one example of the way that patients are gaining autonomy in follow-up care. Health professionals are increasingly able to use real-time data to monitor and support people in the community living with conditions as varied as diabetes, dementia and cancer. Patients with long-term complex conditions can give immediate feedback on how the treatments impact on their quality of life.

The potential is exciting, but there are also dangers, and a need for patients to keep their data safe – especially with the increasing use of apps on mobile phones.

By 2018 there were more than 318,000 health-related apps downloadable from online stores worldwide, with more than 200 being added every day. Most are lifestyle apps: counting steps, monitoring heart rates or sleep patterns, or other proxies for 'wellness'.

On average each app requested four 'dangerous' permissions, such as reading other accounts and noting when the user is engaged in a call

However, about 15% of health apps give patients advice on medication, allow patients to provide feedback, or are designed for health professionals.

They will increasingly be used for two-way traffic – a patient uploads health data to a physician or to a hospital and is then able to download reports or some of their medical records.

The proliferation of apps designed to share this sort of personal medical data is giving rise to concerns. When researchers tested 24 serious health apps they found that, unknown to the user, 19 were sending sensitive information to a remote server (*BMJ* 2019, 364:1920). On average each app requested four 'dangerous' permissions, such as reading other accounts on the device and noting when the user is engaged in a call.

Although data from devices are anonymised, the phone can be uniquely identified, and when two databases are combined anonymity can be stripped away.

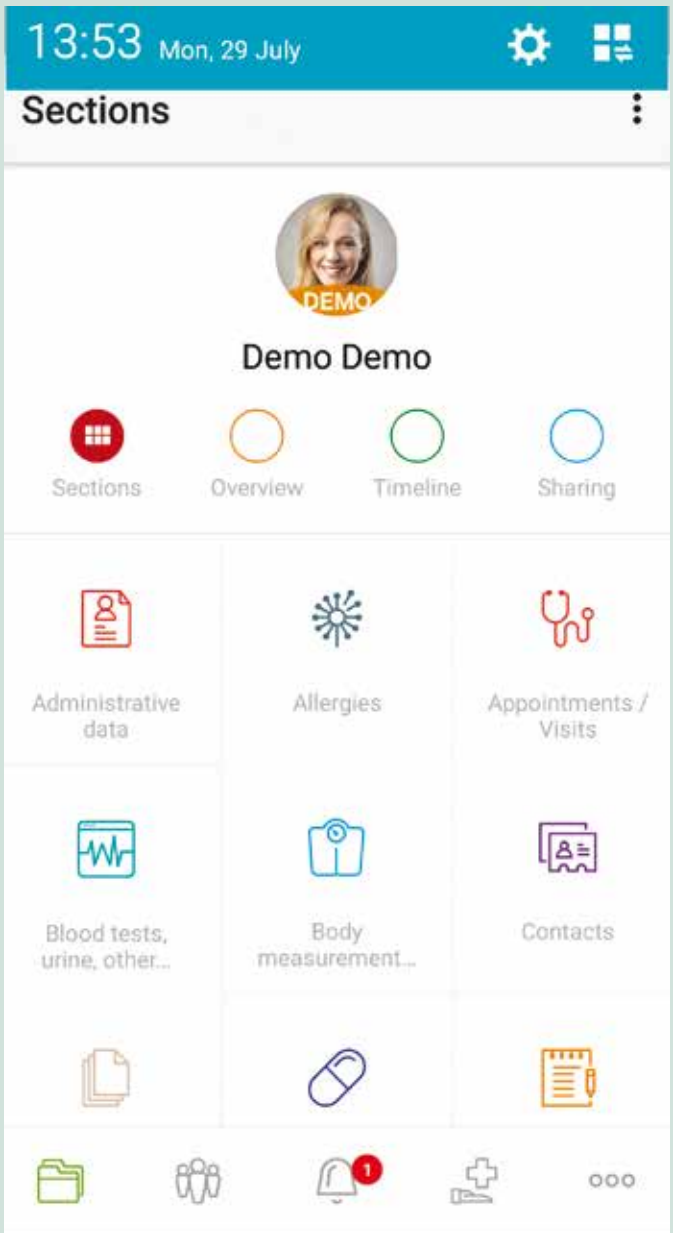
More than 20 years ago, Massachusetts Governor William Weld approved the release of hospital insurance data, reassuring the public that it had been anonymised. Until Latanya Sweeney – now a Harvard Professor, but in 1996 a bright research student – cross-referenced the anonymous data against the electoral register (which includes gender, age and birth date) and sent the shocked Governor his personal health records, including diagnosis and prescriptions.

Today's risks may be no less startling. The authors of the 2019 *BMJ* paper point out that people often download apps without understanding that they are giving permission to collect information on user activity, target advertising and share information with business affiliates. "The lack of transparency, inadequate efforts to secure users' consent, and dominance of companies who use these data for the purposes of marketing, suggests that this practice is not for the benefit of the consumer."

One of the researchers, Ralph Holz, a lecturer in networks and security at the University of Sydney, says that finding ways for patients to protect their data is one of the burning questions of the day. "Even if you are transparent at one point in time and everyone knows what is going to happen with your data, that is not necessarily going to guarantee that the regulation does not change or the company does not change ownership or move to another jurisdiction.

"My hope does not rest with technology. My hope rests with forward-looking policy making and hopefully

When the drive for faster health data became personal...



For Vincent Keunen, getting better and faster cancer treatment and research about cancer is personal. In March 2007 he learned he had chronic myeloid leukaemia (CML). Three months later his ten-year-old son Pierre was diagnosed with Ewing sarcoma.

Vincent Keunen found his way onto a Glivec trial and, 12 years later, now describes his cancer as "a detail" in his life.

His son was not so lucky. Pierre lost his leg and went through two years of intensive treatment. The cancer still affects his life and requires regular check-ups.

Vincent Keunen was a software engineer and businessman with 25 years of experience. He had already developed software widely used in his home country of Belgium to exchange information between hospitals and family doctors.

But he felt helpless and frustrated.

"Glivec is super-efficient and has almost no side effects. CML was deadly before Glivec, with a few months – maximum two years – survival. So it went from a death sentence to no worse than a cold really. At some point I asked how can I contribute to develop new drugs like that, which are so efficient and super-targeted to the disease?"

In his vision, he saw cancer patients pooling experiences to help researchers speed up the search for effective treatments. In real life he saw his son undergoing numerous treatments in different centres that were not properly joined up. "Doctors don't exchange data, they don't have time for that. IT systems don't talk to each other as well as they should. If you go from one hospital to another that is difficult. If you go from one country to another – well …"

He also noted that, when his son had his annual check-up, some tests are repeated several times, when the technology exists for medical staff to monitor things like blood pressure and side effects continuously and remotely.

also with ways for consumers to find redress in case their data has been used in ways that they did not agree to. The big question being how can they even prove how their data has been used unless it is some kind of public leak and someone discloses business practices."

Hospital data sharing systems

Few European hospitals allow patients to access hospital records – but they are making moves to become more connected, aided by developments in the US. As part of 'Obamacare', US hospitals were compelled to introduce an interface (API) to exchange data with the outside world if they wanted to receive insurance money. The US standardised on a protocol called Fast Healthcare Interoperability Resources (FHIR), and that is now

He began to work on a smartphone app – now downloadable as Andaman7 – that would make it easy to share data between patients, healthcare professionals and researchers.

"What drove me to develop Andaman7 initially was the goal of giving patients a way to easily collect data from all sources in a way that is easy for them to use."

"Security by design means that the data does not reside on any server. It is only saved on your smartphone"

He designed it for the phone because that is what everyone carries. At the same time, Keunen recognised that people are wary about allowing personal data to be held in the cloud. The software is designed therefore to hold everything only on the phone, even if the user decides to share with a family member or health professional.

"We follow the GDPR principles of privacy by default and security by design. Privacy by default here means that if you put data directly into Andaman7 it won't be shared with anybody by default. Security by design means that the data does not reside on any server. It is only saved on your smartphone. It is a lot more difficult to hack your phone than to hack a server in the cloud. And even if it was hacked, the pirates would only have access to one record. Not a big deal."

Keunen is also offering the platform to allow pharmaceutical companies to collect real world data from patients on the effects and side effects of treatment.

Currently the Andaman7 app has only been downloaded by about 23,000 patients worldwide, but it is being used and validated in a number of specific projects.

- At the Central University Hospital (CHU) of Liège in Belgium 3,000 patients are using the software to access their medical records – every time they have a hospital visit they automatically receive a report on their phone.
- The Lithuanian National Cancer Patients Association (POLA) is using the software to build a patient-driven registry.
- The EORTC is using Andaman7 to digitise a quality of life questionnaire – currently in two countries and eventually in ten. Patients will have the choice of filling in the questionnaire on their phones or on paper.
- It is being used by a pharmaceutical company to develop a cohort of patients for a clinical trial and by another company to feed data back to patients who have taken part in a trial.

Laboratoires Réunis in Luxembourg, with centres in Belgium, France and Germany, is allowing patients to use Andaman7 to directly download pdf reports on the results of blood or urine tests. Patients will eventually be able to track changes graphically, using the international LOINC standard (a universal standard for identifying medical laboratory and clinical observations).

Keunen believes that being able to access records and input data will improve health literacy, especially for patients with complex conditions like cancer. But he is frustrated at the slow rate at which hospital electronic health records are being opened up to accept patient input.

"Almost no hospital is ready to take in patient data. They need to extend their software, because it is only used by doctors, nurses and health professionals, and you don't even know if it is the doctor or the nurse who entered the data.

"Patients want to be empowered and to know more. If a patient is 45 years old and has had a rare disease for the past 15 years, this guy has been talking to the best specialists and has had lots of hours researching this problem and knows more about this disease than 99% of doctors."

increasingly being taken up in other English-speaking countries and in Europe.

However, clinicians and researchers face major challenges when comparing data collected in different systems. To address this, ASCO published in June 2019 an mCODE initiative – short for Minimal Common Oncology Data Elements.

Richard Schilsky, ASCO Chief Medical Officer, told *Cancer World*: "More than 15 million of individuals with cancer have their data in some sort of electronic health record, but they are prioritised in different ways and the different systems collect data in many formats, making them incompatible with one another. This affects the opportunities for the patients, because their doctors are unable to compare the cases and their outcomes. It also affects the opportunity for research,

especially in the drug domain. We could collect a lot of information on side effects after the official trial ended, if we were able to dig into a large number of electronic health records."

The NHS is now encouraging hospitals to develop their own data sharing systems, which are presumed to have greater local support

Pooling data from many sources opens opportunities to draw treatment lessons from big data but, despite the GDPR data protection regulation, it may lack public trust. The UK NHS suffered a spectacular rebuff a decade ago when the Government decided to pool information from patient records, drugs companies, insurers and others in a new, centralised NHS patient records database. It foundered on lack of trust by family doctors, who were expected to upload patient records, after it became clear that anonymised data would be shared with private companies. The Care.data initiative was put on hold in 2004 and scrapped two years later.

The NHS changed tack and is now encouraging hospital trusts and regions to develop their own data sharing systems, which are presumed to have greater local support. An NHS map of these personal health record schemes shows that cancer services and patients are in the forefront of attempts to improve care.

The Movember Foundation supports the TrueNTH UK self-management and follow-up study led by Southampton University that, amongst other things, allows 2,675 men previously diagnosed with prostate cancer to use an app to access PSA results online, via the NHS-hosted My Medical Records system.

Despite initial concerns that patients saw results before clinicians had assessed them, men were not adversely affected even when test results were abnormal.

There were only slight improvements in outcomes, but high satisfaction levels from patients. And although direct healthcare costs were higher, because the approach includes workshops and support workers, the overall cost was lower because men used fewer health services, and the programme met NICE cost-effectiveness adoption criteria.

This study identified a need to embed patient reported outcome measures (PROMs) in an IT system where patients can be monitored remotely.

Prostate Cancer UK and the Movember Foundation are now calling on all UK health trusts to adopt the programme. Heather Blake, Director of Support and Influencing from Prostate Cancer UK described the approach as "a win–win for cash strapped NHS Trusts".

In another example, the Leeds PPM+ platform connects more than 35 systems across health and social care and has accumulated integrated care records for 2.8 million patients. It began with cancer services in 2003 and broadened out as it proved its worth. Today it links hospital and GP records with hospices, social care and mental health services, allowing clinical and care staff across the region to access vital information about a person's care. It delivers more than 50 million pieces of information every month and is accessed every 3.8 seconds. And in this system patients are able to hold their own electronic records.

As such schemes spread, the NHS has produced a Code of Conduct for those developing apps. This includes the right of patients to opt out of information being used for anything other than individual care and treatment, the need to be fair, transparent and accountable, and the need to 'bake-in' data protection in business practices as well as in software.

However, giving patients the ability to access and input data while keeping them safe from exploitation poses significant challenges, as the European Haematology Association (EHA) is finding, with the development of its electronic monitoring app HM-PRO.

Data security is a concern, and for the time being HM-PRO does not save data or send information from the phone to a server

The aim is to develop a tool that captures patient experiences and makes a measurable difference to clinician decision taking, says Esther Oliva, a haematologist at the

Grande Ospedale Metropolitano Bianchi Melacrino Morelli in Calabria, Italy, who co-chairs the EHA Scientific Working Group on Quality of Life and Symptoms. HM-PRO is already being used in the global Acute Leukaemia Advocacy Network (ALAN) survey to gather information on treatment, experiences and quality of life. It has been translated cross-culturally for use in Europe, China, Korea, Japan and Israel, and will be available in 15 languages within three years.

Significantly, in a study that compared paper and electronic versions of HM-PRO, 87% of patients (average age 63) preferred using the electronic version, which can be downloaded as an app onto their phones. However, data security is a concern for the EHA Scientific Working Group and for the time being HM-PRO does not save data or send information from the phone to a server.

Esther OIiva said that while this clearly protects privacy, the app only becomes fully useful when it connects patients with their clinical teams. "At the moment it is a surrogate for a potential app that might be able to be used in clinical practice, but it requires development to protect patient data. The app should communicate with the server of the health department or hospital, and that is what we are planning to work on."

One of the HM-PRO developers Sam Salek, Professor of Pharmacoepidemiology at the University of Hertfordshire, England, and co-chair of the EHA Scientific Working Group, has a vision where patients use the app to submit reports on quality of life and side effects of treatment into a secure repository, and an algorithm alerts health staff if something appears to be wrong. They use their phones to fill in questionnaires before each outpatient consultation, which can be seen by the clinician in advance and used for joint decision making.

"On the one hand these things have made our lives easier. On the other it has opened a floodgate in terms of abuse of our personal information"

"Use of an app in that sort of fashion to me is really a dream come true – absolutely revolutionary.

"As healthcare professionals we don't have very much access to what the patient knows. We know the clinical diagnosis and a bit about the treatment but not the non-medical factors which are the patient's expertise. The patient's full engagement is absolutely vital."

Salek does not fear that patient data will leak from hospital systems protected with firewalls, or from trials where data is encrypted and anonymised. "I don't think that any of the data of patients taking part in any clinical trial or any sort of observational study or real world data use is abused."

He agrees, however, that despite GDPR many commercial phone apps are not secure. "When we accept their cookies as we access the website, then they can trace all our activities on the internet. We are dealing with a double-edged sword. On the one hand these things have made our lives easier. On the other hand it has opened a floodgate in terms of abuse of our personal information and theft of our identity."

Sophie Wintrich, chief executive of the MDS UK Patient Support Group, for patients with myelodysplastic syndrome, collaborated in the development of HM-PRO, because she could see it was being developed entirely with patient interests at heart. But she has noticed an increase in older patients using phones and tablets to access information about their condition, and wonders how aware they are about possible leaks from other apps.

"People with a disease are vulnerable because they are desperate for contact with other patients, and desperate for information for assistance, and they may overlook the fact that not all of the sharing platforms that are available provide you with the safety that they should.

"You have platforms where patients are invited to put in their details about their quality of life but also their co-morbidities or some personal data, and they are not fully transparent in terms of who funds the tool and what happens to the personal data.

"You also hear of situations where data of patients has been sold to insurance companies or to pharma companies. Smart phones in the hands of people who do not necessarily read the terms and conditions is potentially quite dangerous There is no proper informed consent unless information is fully transparent."

To comment on or share this article, go to bit.ly/CW87-PatientData