Digital technology: How to get it right - Data governance, storage of data, and the regulations

W Angus Wallace, Phil Booth and DJ Hamblin-Brown

Angus Wallace developed an interest in informatics while carrying out his shoulder research in 1984. He created the Faculty of Medical Informatics at the Royal College of Surgeons of Edinburgh in 2000 and was appointed Dean of Clinical Informatics from 2000 to 2005. He has subsequently become a Founding Fellow of the UK Faculty of Medical Informatics (2017) and is Chair of the FCI UK Events Organising Committee (2019-23), running their three Annual Scientific Conferences to date. He continues reviewing papers for his main clinical interest - shoulder surgery having been a past President of the British Elbow and Shoulder Society (2001-3) and President of the International Conference of Shoulder and Elbow Surgery (Edinburgh 2010).

Digitisation of health records is now a routine part of our medical practice. We need to learn the rules and follow the rules, but what are the current rules?

What are the current rules on patient data information?

UK rules around health data are complex, arising from several bodies of law, including Common Law (confidentiality), various NHS and Health Acts (most recently the Health and Care Act 2022, but importantly also the 2002, 2006 and 2012 Acts) as well as all personal data falling under the UK Data Protection Act (2018) and UK GDPR[1].

Data protection law requires that all personal data should be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

ENCRYPTION
All digitised confidential information should be protected via firewalls, passwords & encryption

Figure 1: All digitised confidential information should be protected via firewalls, passwords and encryption.

There are stronger legal protections for more sensitive information, deemed ‘special category’, which includes information pertaining to:

Race; ethnic background; political opinions; religious beliefs; trade union membership; genetics; biometrics (where used for identification); health; sex life or orientation.

These rules are enforced by the Information Commissioner, in cooperation with the National Data Guardian in England, who has legal competence and expertise

Phil Booth coordinates medConfidential, which campaigns for confidentiality and consent in health and social care, seeking to ensure that every use of data across and around the NHS and wider care system is consensual, safe and transparent. Founded in early 2013, medConfidential works with patients and medics, service users and care professionals, drawing advice from networks of experts across the UK and around the world. Phil previously led NO2ID from 2004-2011, campaigning successfully to defeat the introduction of ID cards and other 'database state' initiatives. His work as an advocate has been recognised by awards from Privacy International (2008) and Liberty (2010). Phil was an honorary research associate of the School of Psychology at the University of Birmingham from 2002-2012, and he advises a number of organisations seeking to provide individuals with more meaningful control over their own personal data.

Dr DJ Hamblin-Brown, FRCEM, MFCI has had a career which spans medicine, information technology, consulting and healthcare advisory roles. He has spent most of his clinical years in Emergency Medicine, including several years at consultant level in a large NHS trust. Pre-pandemic he was VP Medical Affairs for a group of seven acute-care hospitals across China and prior to that Group Medical Director of Aspen Healthcare in the UK. He is now the CEO of CAREFUL.online Limited, which has designed and markets handover and patient flow software.

in non-data protection rules and practices. All organisations or individuals who hold personal information are legally required to register with the Information Commissioner's Office (ICO). If you are an NHS employee, NHS bodies are registered with the ICO, however if you hold patient information outside the NHS platform you are required to legally register with the ICO personally. These are not your only lawful obligations – there are many other rules you can break too[2] – but full compliance with data protection law is a baseline.

What are the current rules on transferring patient data?

These are determined not only by primary legislation but by regulations, policy, institutional systems and practices, and professional ethics. As stated above, patient data should be "handled in a way that ensures appropriate security" – and which you can show meets all other lawful and professional obligations as well.

For any processing of data – and more particularly for sensitive information, including health data – the patient needs to give consent. NHS trusts rely primarily on the 'implied consent' given by seeking medical attention. Independent hospitals will often gain explicit consent during the registration process.

What platforms are acceptable for the transfer of NHS patient data (including radiographs and images)?

The NHS has produced its own repository for patient data and each NHS Trust has Information Officers, Data Protection Officers and Caldicott Guardians who oversee the way data is stored and used. We are all now knowledgeable about the Picture Archiving and Communication System (PACS) and these have become easier to use and more integrated across regions. However, by expanding these systems they are potentially more vulnerable to unauthorised uses by authorised users, as well as access by those who are not legally allowed permission to access this information. There are monitoring systems in place that identify and log anyone accessing personal patient data via their login and password. Therefore, you will be placing yourself at personal risk if you share your login and password with others – this breaches the rules.

What about the filing cabinet in my office? Or my personal computer

In general, you should not store or process information personally – even if it's anonymised – unless you are in practice for yourself. Different, and more strenuous rules apply to research data. If you want – or need – to store any information on your computer or on paper, then you need to be registered with the ICO. A small yearly fee applies. If you do this, you'll need to have written policies about what you store, how it's protected and how long you keep it. Any staff you employ will need to evidence that they understand and comply with these policies. You'll also need to ensure you get patient consent for anything you store. Failure to do this can result in hefty fines. Losing a briefcase of clinic notes will put you in serious hot water.

What about using WhatsApp during COVID?

During the COVID pandemic, NHS rules were 'relaxed' to facilitate the better management of patients in a crisis situation; these pandemic operating conditions were extended to June 2022[3]. Before COVID, official guidance on the use of apps like WhatsApp was unclear. During the pandemic – as with other platforms, such as for video consultations – WhatsApp was allowed to be used but only if the amount of personal/confidential patient information transmitted is 'minimised'[4].

It is currently known that some NHS staff are breaking these rules and could be disciplined so our recommendation is – please stick to the rules. Many doctors have found WhatsApp invaluable, particularly when sharing images with experts outside their NHS region. >>

NHS regulators approve the use of WhatsApp during emergencies

NHS England has published guidance on the use of instant messaging apps during emergencies.

Figure 2: https://nursingnotes.co.uk/news/nhs-regulators-approve-the-use-of-whatsapp-during-emergencies. *Please note this guidance has now been cancelled.

Doing this on a one-to-one basis, ensuring images are as de-identified as possible, is acceptable because WhatsApp is 'end to end encrypted'. A WhatsApp group is a completely different situation where you, as the sender, have no control of all the recipients, any of whom could download and distribute a WhatsApp message or image. This has been the downfall of a number of Members of Parliament in recent months.

On the whole, however, the use of messaging apps is unlawful since patient consent has not been gained for the use of data in this way. Bear in mind that despite encryption in transit, WhatsApp data can be read by Meta, the parent company of WhatsApp and Facebook. The data sits on a server somewhere. You have been warned!

How long should I keep patient data

If you're storing patient data, you need to ensure that all data is retained for the appropriate length of time. This is laid down by the NHS Records Management Code of Practice. The short answer is eight years for adults and 25 years for children.

The Control Of Patient Information (COPI) Notices

The COPI Notices were an emergency measure that required and provided the legal basis for much greater sharing of healthcare data during the COVID pandemic. These rules quietly came to an end (mostly) on 30 June 2022[5]. This has resulted in a number of potential breaches of confidentiality possibly now taking place and it is important for doctors to be aware of these changes and seek advice from the appropriate Clinical Information Officer and/or Information Officer, Data Protection Officer or Caldicott Guardian at their own place of work.

A plan for digital health and social care

On 15th June 2022, following the April publication of the Goldacre Review[6] it had commissioned, the Department of Health and Social Care published its ***data*** strategy, 'Data Saves Lives'[7]. And on 29th June 2022 the Department of Health published its plan for ***digital*** health and social care[8]. This summarises where the Department and NHS England believe data and digital in the NHS should be going over the next 10 years. The plan is ambitious, but likely not achievable with – amongst other factors – the financial constraints being applied to the NHS and the Social Care sector. In essence, the short-term plan is to 'bust the backlog' by making hospitals more efficient, by spending £8 billion on more IT. Better handovers and better patient flow through secondary care would of course help, but if the Government and NHS England have their way, a more profound restructuring is about to take place.

New NHS-developed software

In the meantime – in line with Professor Goldacre's key recommendation that the NHS adopt "modern, open ways of working", investing in people and open, reusable code – much work has been carried out on developing compliant patient information software suitable for doctors sharing patient data. One of the authors (WAW) is aware of an excellent project carried out by Helen Craggs at the Royal Bolton Hospital[9] where an automated electronic Acute Medicine Referral List (AMRL) was developed that 'talked to' their Allscripts™ Electronic Patient Record. A commercial system, CAREFUL.online, has been developed by one of the authors in order to facilitate safer handover within and between teams, replacing poorly compliant handover sheets[10].

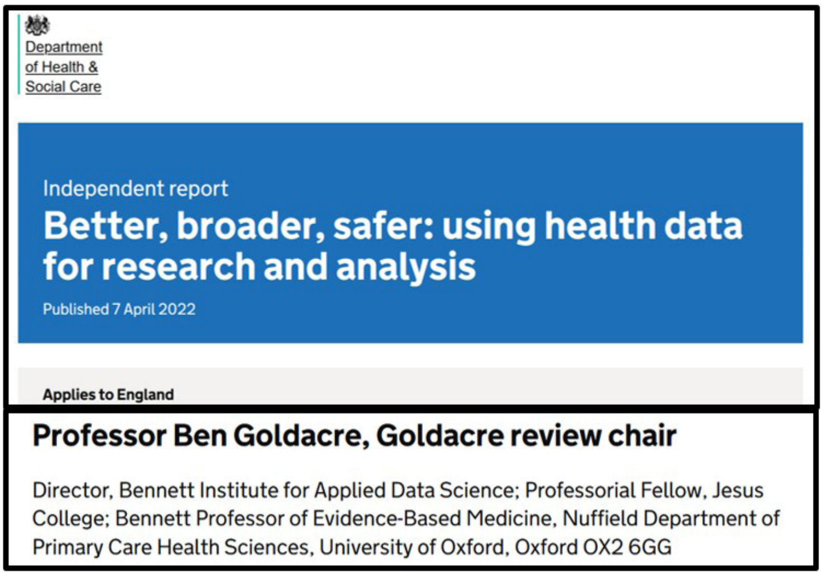
Good principles for sharing patient data

While the law and rules may appear (and can be) complex, most issues around the processing and sharing of patients' health information can be addressed by following three straightforward principles. It is these principles on which medConfidential has been campaigning since 2013, i.e. that every use of patients' data should be **consensual**, **safe**, and **transparent** – noting that *consensual* does not always mean prior informed *consent*; it covers bases such as well-communicated, functional opt-outs, specific statutory exemptions, and implied consent for direct care.

With the adoption of Five Safes[11] 'Trusted Research Environments', which parts of the NHS call 'Secure Data Environments', and robust equivalents such as OpenSAFELY[12] under appropriate post-COPI governance for *patient-dissent able* research and planning uses, by NHS bodies and others, the future looks much safer than it has been. And, as each past attempt to hoover up patients' data for non-care purposes has failed to do, patients must be told how their information is used.

We can only hope that as the latter takes over the former, the culture and practices of transparency developed and demonstrated by NHS Digital over the past several years will 'infect' NHS England, whose institutional secrecy – both during the pandemic and before – has proven toxic to public trust, time and again.

Meanwhile we can all work together, holding ourselves accountable for what we do with the data we use; demonstrating the same respect we afford the people from whose lives it is abstracted. ■



Department of Health & Social Care

Independent report

Better, broader, safer: using health data for research and analysis

Published 7 April 2022

Applies to England

Professor Ben Goldacre, Goldacre review chair

Director, Bennett Institute for Applied Data Science; Professorial Fellow, Jesus College; Bennett Professor of Evidence-Based Medicine, Nuffield Department of Primary Care Health Sciences, University of Oxford, Oxford OX2 6GG

Figure 3: www.gov.uk/government/publications/better-broader-safer-using-health-data-for-research-and-analysis/better-broader-safer-using-health-data-for-research-and-analysis.

References

References can be found online at www.boa.ac.uk/publications/JTO.