Life & Times Special Series

Confidentiality, privacy, and general practice:

GPDPR and the brave new world of 'big data'

INTRODUCTION

Big data is big business. Health data is valuable for the public good — it can save and improve lives — but it can also be monetised for private profit. The UK's NHS data has been valued at £10 billion. GP data — with details of everything from medications to diagnoses that include mental illness, abortions, sexually transmitted diseases, suicide attempts, and addictions — is arguably the most detailed, valuable, and sensitive of all. Health data provides the fodder for machine learning, a subfield of artificial intelligence, that some argue will revolutionise health care, making it more efficient and effective. But ultimately, data emerges from the stories and information that patients bring to healthcare professionals and how these are interpreted, recorded, and acted on. This means that we should give careful consideration in incorporating patient and public views in the decisions made about their data. We should also consider whether an excessive focus on digital data may blind us or distract us from the valuable 'data' that patients as whole human beings bring to the consultation — their values, feelings, relationships, unique life stories, and particular circumstances. Nor should it belittle the importance of relationship-based care.

WHAT IS GPDPR?

GPDPR, GP Data for Planning and Research — not to be confused with GDPR — General Data Protection Regulation (which is about protecting not sharing your data) — is set to happen on 1 September 2021, having been (briefly) paused from the earlier date of 1 July after criticisms from various institutions including the British Medical Association and Royal College of General Practitioners, as well as a threat of legal action. The GP data from 55 million people will be 'pseudo-anonymised', but can in fact be readily de-anonymised, according to data experts. Many GPs — the designated 'data processors' who carry the responsibility to inform and seek consent from their patients — are deeply concerned. In fact, many of us have a *déjà vu* of care.data, but alarmingly, the planned mining is deeper and wider than in 2014. Information provision and genuine consultation with the public has been minimal. In fact, it is highly likely that the great majority of the public are unaware of the planned extraction.

CONFIDENTIALITY AND CONSENT

Medical confidentiality has a long and venerable history and is a key tenet of professional codes of ethics, from The Hippocratic Oath (over 2500 years old) to the current guidance for doctors' duties from professional bodies such as the General Medical Council and the World Medical Association. Confidentiality is considered an essential element for gaining and sustaining trust. It is not absolute and other ethical and legal considerations may supersede, but this does not mean it can be ignored or should be overridden by ill-defined utilitarian considerations of the 'public good'.

GPDPR raises ethical and legal issues around confidentiality and consent. Having practised as an NHS GP in London for 35 years, I am only too aware of the very personal and intimate nature of the information that patients offer me. As GP's we bear witness to the stories our patients bring us. We listen to tales of sexual and physical violence, of secret fears and aspirations, of crushed hopes, of anger and despair, of hidden love and addictions. Often these are accompanied by the statement *'I have not told anyone else, doctor'* or *'This is the first time I have spoken about this.'* We also listen to more mundane stories, or stories of stoicism, of courage, of unswerving loyalty and awe-inspiring altruism. These conversations are held in the context of a trusting relationship on the assumption that the information given will not be shared beyond those who are involved in their care.

Given this situation, it is undeniable that patients should be given the opportunity to decide who has access to their data and to what purposes it will be used. This shows respect for persons and their human rights, such as protection of private and family life from an intrusive state, as highlighted in the Nuffield Council on Bioethics 2015 report on biological and health data. Furthermore, consent does not mean control: it does not allow for data subjects to fully determine the aims or

Paquita de Zulueta

purposes of the use of their personal health data, or to control data access agreements, or to specify sanctions for breaches. It does not allow for decision-making power or agency. 'Research and planning purposes' can cover many activities, some of which they may not approve of.

A government also has a legal and moral duty to consider the impact on people's rights and to meaningfully engage with the public when planning to process health data on a national scale. So far, we have not seen impact studies and there has been scarce attempt from the government to inform, let alone engage, with the public on this issue, although the Wellcome Trust's *Understanding Patient Data* initiative has undertaken public attitudes and engagement research.

DEFINING 'PUBLIC INTEREST'

'Public interest' or 'public good' are malleable, subjective concepts yet they can be applied with the full force of the law. Access to health data without consent is possible via section 251 of the NHS Act 2006 such that the common law of confidentiality is set aside for various purposes such as clinical audit, research, or healthcare management, which are deemed to be in the public interest, such

> *"... conversations* [with patients] *are held in the context of a trusting relationship on the assumption that the information given will not be shared beyond those who are involved in their care."*

as improving patient care.

The trope of pitting social or public good against the individual's right to privacy creates a false dichotomy. For example, if patients cease to trust their clinicians, public good will suffer. Furthermore, a large body of research investigating public attitudes towards sharing health data has found that people approve in general for their data to be used for medical research and for 'good causes', whether environmental, social, or medical, but do not approve of their data to be used for commercial purposes or for powerful companies to profit at society's expense. They also want it to be privacy-preserving, trustworthy, to have some control of the purposes it is used for, and for the freedom to opt out.

COMMERCIAL INTERESTS?

Given that sensitive health data from NHS hospitals has been shared with or sold to 29 separate commercial companies in the last year (and 43 in the past 5 years) and there is a lack of audit trails tracking further use of data, reassurances that the data will only be harnessed for public benefit and not sold to private companies for profit do not inspire confidence or allay doubts. Disturbingly, there is also evidence that pharmaceutical companies have exploited the data to price drugs being sold to the NHS and that, once taken, companies have blocked NHS access to its own data.

We also know that the NHS has links with commercial technology giants and the corporate sector. For example, NHSX holds the extensive NHS COVID-19 datastore, which has contracts with Palantir Technologies, a US company known more for supporting spy agencies, militaries, and border forces, as well as with Amazon, Google, and others to provide data analysis and management. How aware is the public of this and how comfortable are they for these companies to have access to their medical data, even with safeguards? Sarah Cheung argues persuasively that the 'trade-off fallacy' and 'obfuscatory practices' negate individuals' control of the future use of their personal health data and enables widespread involvement of commercial actors in accessing and using personal data. Consumers can withhold their data from companies they do not approve of, but patients or service users cannot avoid seeking health care and are therefore disempowered and more vulnerable to exploitation.

GP DATA: WHY IT IS DIFFERENT AND WHY THAT MATTERS

A key feature of general practice is that GP's regularly work in the context of uncertainty and complexity. Patients' narratives are often vague and/or ambiguous. Diagnoses emerge over time, but not always. Roger Neighbour, in his insightful book *The Inner Physician*, highlights the flaws in the traditional medical model of diagnosis and the disproportionate reliance on physical text. He points out that this model fails to recognise the interconnectedness of causal factors and how the process of questioning can change the story that is elicited. Over-reliance on digital data carries the same risks of distortions and over-simplifications. Qualitative researchers found that when confronted with vague, unfamiliar symptomatology, GPs are very reluctant to code with specific Read codes and will opt to not code at all or to use a very generic code. This understandable lack of specificity is anathema to those who want precision, predictability, and control.

The stories patients bring us — often filled with ambiguity and uncertainty — have to be fitted into the Procrustean bed of accurate, reliable codes compatible with research and public health agendas (unless of course free text is uploaded as well, thus further invading privacy). Read codes have now been ditched for SNOMED because the former were based on a 'GP viewpoint' and lacked 'semantic accuracy'. The GP perspective, we are told, never worked well in a hospital setting 'as consultants and specialists have a very different view on a healthcare problem.' Implicit in these remarks is a disparagement of the 'GP perspective', as Neighbour also comments on and vigorously rebuts.

TRUST AND ACCOUNTABILITY ARE DIFFERENT ENTITIES

Trust is crucial and should not be assumed in the healthcare context. The philosopher, Onora O'Neill, in her Reith lectures on trust, is highly critical of the use of accountability and transparency as surrogates for trust. She argues that these may in fact undermine professionalism, honesty — and trust. To trust requires accepting uncertainty and risk, a belief that those in whom one has placed one's trust are trustworthy — they have our best interests at heart and can be relied on to behave virtuously. Ensuring that systems are secure and not liable to be misused, hacked, or corrupted is a matter of reliability, not of trust or trustworthiness, although it is undeniably important. Caldicott Guardians, GPs, and clinical researchers hold a duty of care and need to be trustworthy. But the key question is: *who has the power to control what happens to our health data? And do we trust them?*

DATA STEWARDSHIP

Data stewardship is a concept that is gaining ground. The Ada Lovelace Institute (ALI) define data stewardship as *'The responsible use, collection and management of data in a participatory and rights-preserving way.'*

Data can be considered as part of the 'commons' — a public good to be shared within a framework that prevents a free for all. Data differs from concrete goods as it is 'intangible' and can be reused limitless times, making it both more valuable and subject to exploitation. The ALI adapt for the purpose of data sharing the late economist Elinor Ostrom's eight rules for managing the commons. The Nuffield Council on Bioethics' recommendations also emphasise respect for human rights, regular engagement and communication with the public, and stringent regulatory procedures including reporting security breaches and departures from stated aims.

CONCLUSION AND FINAL THOUGHTS

With our increasing reliance on digital infrastructures, machine learning, and data, we need to ask ourselves what kind of health care will we have and is it what we want? General practice appears to be at a crossroads: it could submit to the current hegemony of a utilitarian, disease-orientated, 'data-driven' model of health care or it could strengthen its core praxis: relational, person-centred, holistic care underpinned by an ethic of duties, reciprocal rights, and virtues — in particular, compassion and practical wisdom — combined with a solid understanding of the social determinants of health. Hopefully it will find a way of balancing the two.

So, I throw down the gauntlet here: I cannot see how GP's, in good conscience, can agree to the wholesale upload of their patients' 'data' without being confident that their patients have given valid consent, that we know who will use it and to what purposes, what protections and responsibilities will be in place, and whether there will be an ongoing authentic — not tokenistic — public participation in the sharing of health data.

'Data' derives from the Latin *dare*, 'to give', and it behoves us to acknowledge and respect those who offer us their gifts in a spirit of trust.

Paquita de Zulueta,
Paquita is a retired GP still actively teaching and writing about medical ethics and compassion in health care, coaching and mentoring doctors, and acting as a Schwartz Rounds facilitator.
Email: p.dezulueta@imperial.ac.uk
@PdeZ_doc

This article was first posted on *BJGP Life* (with full reference list) on 4 August 2021; https://bjgplife.com/confidential

DOI: https://doi.org/10.3399/bjgp21X717017