ENSURING THE EFFECTIVE USE OF PATIENT DATA

The effective use of patient data is of critical importance to improving healthcare delivery, service design and medical research in the NHS. Information from patient records has huge potential to save and improve lives but the need to protect patient privacy must be taken seriously. We are becoming increasingly concerned that lessons from the failure of the care.data programme have not yet been adequately addressed. There is a real risk that the mistakes will be repeated unless the following actions are taken:

1. There must be clearly defined and transparent governance processes, with a single and coherent overarching framework for accessing patient data.

2. There must be robust and proportionate safeguards. The 'one strike and you are out' principle, for example, is still not enshrined in legislation and further work is needed to develop appropriate requirements for secure data facilities and accredited safe havens

3. There must be absolute clarity about the purposes for which data can – and cannot – be accessed, with transparent guidance about acceptable and unacceptable uses.

4. A single, coordinated communication strategy with clear information to reach the widest possible audiences, is essential. There is a danger that competing dialogue processes from care.data and NIB will exacerbate confusion.

5. There must be absolute clarity about the opt-out process.

6. As part of strengthening safeguards, more meaningful sanctions for re-identification could be introduced into legislation.

This briefing sets out further background about each of these points, and recommends actions to address them. When asked, most patients support the idea that information about them can be used for purposes other than their immediate care. Many are positively keen for this to happen, but only under properly controlled conditions with respect for their privacy. It is essential that governance processes provide assurances to the public, healthcare professionals and the research community that data access is being appropriately managed. Without these safeguards in place, it will not be possible to build trust in the system.

1. There must be clearly defined and transparent governance processes

- There are an increasing number of bodies involved in discussions about data access, including the Department of Health (DH)'s National Information Board (NIB), the National Data Guardian and the Independent Information Governance Oversight Panel, the HSCIC and its various information governance and access committees, the Health Research Authority's Confidentiality Advisory Group (CAG), the MISG External Reference Group, and NHS England's care.data programme – to name but a few. The complexity of the landscape leads to confusion, and increases concerns about inconsistencies and contradictions.
- There is also an increasing risk of fragmentation, with the creation of different processes for the use of data for commissioning, audit and research purposes.
- There must be a single and coherent overarching framework for accessing patient data for uses beyond immediate care. A transparent and proportionate approach that can be applied to any use of patient data is critical to build a trustworthy system.
- A clear diagram of information flows and processes, describing the role of different advisory bodies and key decision-making points at each stage would be a helpful step forward.
- Discussions about health data need to take place in the context of wider discussions about 'big data' and the use of data technologies; these conversations must be joined-up.

2. There must be robust and proportionate safeguards

- We recognise that risks to privacy cannot ever be entirely eliminated but they must be effectively managed.
- The HSCIC is developing the concept of a Secure Data Facility for the care.data pathfinders. However, the current proposals are not scalable beyond the pathfinders, and do not apply to researchers. A workable system, building on the approach developed by the Administrative Data Research Network, will be critical.
- In the meantime, researchers have experienced significant delays, often of more than a year, when trying to access data from the HSCIC.[1] In some cases, researchers have not been allowed access to data even where participants have consented to the research, or where the data requested are at an aggregate level had have been through anonymisation processes. A wide range of research has been affected, including clinical trials, cohort studies, research for health services planning, and audit and evaluation work. HSCIC must continue to work with the research community to address the backlog of applications, to provide consistency and clarity

[1] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/health-committee/handling-of-nhs-patient-data/oral/17740.html

in decision-making, and to understand better the needs of the research community when developing new requirements.

- DH consulted on a system for Accredited Safe Havens in April 2014, but there was little clarity about what uses the proposals were intended to cover. We are still waiting for the Government's response to the consultation.
- The Government has made frequent statements that the principle of 'one strike and you are out' has been enshrined in legislation for all data access requests. However, this was not actually included in the Care Act 2014; Lord Howe in the House of Lords debate on 7 May stated that "the intent is also that the regulations would create a 'one strike and you are out' deterrent to discourage the misuse of these data." We are still waiting for the CAG regulations to be laid; if the provision is included it will be something that CAG would be required to take into account in its advice to the HSCIC on the dissemination of data that might be used to identify an individual. There is therefore scope for flexibility within this provision, and it would presumably only apply to requests on which CAG provides advice.[2]

3. There must be absolute clarity about the purposes for which data can – and cannot – be accessed

- Public attitude work repeatedly demonstrates that the public's main concern about secondary uses of data is about commercial access to personal information. Revelations in 2014 indicated that Hospital Episodes Statistics data had been given to the Institute and Faculty of Actuaries for insurance purposes, despite assurances this would not be possible. There must be absolute transparency as to who can access data, and for what purposes.
- In light of these concerns, the Care Act 2014 set out the purposes for which HSCIC can disseminate data, for:

  (a) the provision of health care or adult social care, or
  (b) the promotion of health.

  The explanatory notes made clear that this would enable data to be made available for the commissioning of health services, and for epidemiological research. It also specified that data could not be used "for solely commercial purposes such as for commercial insurance".
- However, these broad definitions have not given the public and patients the confidence needed that their data will be used appropriately. There is very little explanation of the breadth of basic research that should be allowable. Of more

[2] Lord Howe, Hansard, 7 May 2014: First, he asked about the "one strike and you're out" intention to which I referred. We believe that this will be a criterion that the Confidentiality Advisory Group, the CAG, will take into account in its advice to the HSCIC on the dissemination of data that might be used to identify an individual, so there is already scope for flexibility and common sense within this provision. We anticipate that the transparency of the information centre's decisions to release data, which is provided for in the 2012 Act, would provide further safeguards and reassurances that a "one strike and you're out" rule was being used appropriately—so there is flexibility. This is one matter on which NHS England in particular will want assurance as the engagement exercise proceeds, as will Ministers."

concern, 'promotion of health' could be taken to broadly encompass health promotion, which could include using data from the HSCIC in marketing campaigns or, for example, by the food industry to target healthy eating promotions.[3]

- We were given reassurances by DH that acceptable – and not acceptable – purposes would be defined more clearly, but this has not yet happened. While we recognise that it would never be possible to draw up an exhaustive list, we do believe there needs to be much clearer guidance about the purposes for data can and cannot be accessed in order to restore trust. There must be no surprises about how health data can be used.
- The Wellcome Trust has commissioned some work to examine public attitudes to commercial access to health data in more detail. We hope this work, which is due to be published in January 2016, will help inform policy-making in this controversial area.

4. A single, coordinated communication strategy with clear information to reach the widest possible audiences, is essential

- This must provide information about how patient records are used beyond direct care, the benefits and risks of using patient records, the safeguards that are in place and the opportunities for people to make an informed choice about how their data might be used.
- Any communication strategy must also engage healthcare professionals. GPs are the data controllers; it is essential that they can have confidence in the governance processes and feel able to discuss the benefits and risks with their patients.
- We are concerned that the care.data programme is planning to go ahead with communication to the pathfinder practices, while NIB are also planning a national dialogue. This risks creating further confusion. A single, joined-up communication setting out all potential uses of data and describing an overarching governance processes would help give patients confidence that their data are being respected.

5. There must be absolute clarity about the opt-out process

- We do believe an opt-out system is the right approach. The more people who allow their data to be shared, the larger the dataset and the better the research that can be conducted. With an opt-in system, numbers would be much lower because very few people would take the steps required to actively opt-in. There is a risk that a skewed dataset would be created as a result, which would lead to a potentially dangerous

[3] Lord Howe, Hansard, 7 May 2014: "Health promotion purposes would include wider public health purposes such as research into environmental factors associated with asthma, or for healthy eating."

bias in research results. There are particular concerns about the representation of low socio-economic groups and ethnic minorities.[4]

- For an opt-out system to be meaningful and ethical, it must be accompanied by appropriate information, explaining both potential benefits and risks, to enable people to make an informed decision. We recognise that care.data has recently made significant progress in developing a clearer opt-out form for the pathfinders.
- However, there is still significant confusion about the opt-out process, whether there are one or two opt-outs and whether there will be any impact on direct care, for example in relation to invitations for screening programmes. One of the main difficulties is that care.data programme relates to one very specific extraction of data, but people are looking for clarity across the whole of the healthcare system. There is not yet an option to opt-out from HES data. This needs to be urgently resolved.

6. As part of strengthening safeguards, more meaningful sanctions for re-identification could be introduced into legislation

- We recognise that no system will ever be 100% secure, but it is important that any potential for risk of re-identification is effectively reduced and managed.
- Criminal sanctions for unauthorised and unwarranted re-identification of pseudonymised medical data would be one of the most powerful available methods of managing this risk. A criminal penalty for re-identification would provide a stronger deterrent than the system of fines currently in place for the Information Commissioner.
- This should be introduced across all uses of data, and focus on the intent behind any attempted re-identification. Clarity over the law and appropriate training will be essential to ensure suitable implementation; the intention is not to create a very risk averse culture that would undermine attempts to share data appropriately.

For further information, please contact:

Nicola Perrin, Head of Policy, Wellcome Trust
Tel: 020 7611 8646 email: n.perrin@wellcome.ac.uk

[4] See, for example, a case study on breast cancer care documented in the Academy of Medical Sciences' 2011 review of research governance, Box 6.1: http://issuu.com/acmedsci/docs/newpathw