Department of Health: Protecting Health and Care Information A consultation on proposals to introduce new Regulations

The J Kenyon Mason Institute for Medicine, Life Sciences and Law is an interdisciplinary research network based at the University of Edinburgh.[1] Located within the School of Law, the Mason Institute (MI) aims to investigate the interface between medicine, life sciences and the law in relation to technical, social and ethico-legal issues.

MI welcomes the opportunity to submit evidence to the Department of Health's Consultation on 'Protecting Health and Care Information: A consultation on proposals to introduce new Regulations' (hereinafter 'Consultation'). Members of the MI Executive Committee led the information governance research stream of the ScottisH Informatics Programme (SHIP), funded by the Wellcome Trust.[2] Professor Graeme Laurie and Nayha Sethi produced the Good Governance Framework (GGF) for SHIP which began operations in 2012. The GGF sets down standards according to which the initiative operates and citizens' privacy is appropriately protected. As well delivering proportionate governance within key areas of NHS Scotland, the GGF also served as the basis for the Scottish Government's public consultation on cross-sectoral linkage.[3] Three additional projects undertaken by members of the MI Executive also focus on the regulation of health and non-health data. These projects are:

[1] The J Kenyon Mason Institute for Medicine, Life Sciences and Law <http://masoninstitute.org/> accessed 23 July 2014.

[2] This work was supported by the Wellcome Trust through the Scottish Health Informatics Programme (SHIP) Grant (Ref WT086113). SHIP is collaboration between the Universities of Aberdeen, Dundee, Edinburgh, Glasgow and St Andrews and the Information Services Division of NHS Scotland. For more information see: <http://www.scot-ship.ac.uk/> accessed 23 July 2014.

[3] See, for example, the Scottish Government Consultation here: http://www.scotland.gov.uk/Publications/2012/03/3260/4 or http://tinyurl.com/nepbmfq. Also, seethe Scottish Government Strategy and Guiding Principles for Data Linkage (ISBN: 9781782562047): http://www.scotland.gov.uk/Publications/2012/11/9015/1 or http://tinyurl.com/nw52myj.

- the ESRC-funded Administrative Data Research Centre-Scotland;[4]
- the 10-funder consortium led by MRC on the Farr Institute (Scotland);[5] and
- the Wellcome Trust Senior Investigator award project on Confronting the Liminal Spaces of Health Research Regulation, commencing in October 2014.[6]

Our interests in the proposed Regulations centre on:

- the extent to which the Regulations could promote and facilitate appropriate, scientifically sound health-related research whilst maintaining a robust yet proportionate level of governance, in recognition of the specific risks and benefits of any proposed use of health data;
- the extent to which the Regulations would recognises the public and private interests in protecting the privacy of individual data subjects *and* the important public and private interests that can be served by legal, ethically sound and scientifically robust use of data for research in the public interest.

It is from these perspectives that we address the following questions in the Consultation.

Purposes

Q1. Are these purposes the right ones? Are there any other purposes that it is acceptable for an ASH to use data for? Please set out what you think the purposes should be.

A key element of SHIP's GGF is *principled proportionate* governance.[7] This implies that any regulatory checks and balances imposed within a governance framework should reflect the actual risks involved, should clearly identify the range of purposes to be delivered and should do so in a manner that is not unduly onerous or overly complex. We question whether the purposes set out in the proposed Regulations would, in fact, further fragment the already complex legal landscape for the processing of health data and the lawful bases upon which use of health data may be legitimately used to promote health-related research.

[4] Administrative Data Research Centre-Scotland <http://adrn.ac.uk/centres/scotland> accessed 23 July 2014.
[5] The Farr Institute @ Scotland <http://www.farrinstitute.org/centre/Scotland/3_About.html> accessed 23 July 2014.
[6] Wellcome Trust Liminal Spaces Project: WT103360MA: <http://www.law.ed.ac.uk/research/research_projects/sites/wellcome_trust_liminal_spaces> accessed 23 July 2014.
[7] Graeme Laurie and Nayha Sethi, 'Towards Principles-Based Approaches to Governance of Health-related Research using Personal Data' (2013) 4 The European Journal of Risk Regulation 43–57.

For example, it is not clear where health-related research would fit amongst the current stated purposes laid out in para 26. This is especially important in light of s.111(2) of the Care Act 2014 which specifically lays out obligations for the Health Research Authority (and other agencies) to encourage and facilitate ethical research.

We also note with some concern the use of the phrase 'between population groups' (para 26). This begs the question of whether research *within* a population group would fall under the purposes set out. If the current structure of 'purposes' is to be retained, we would recommend redrafting to 'within or between population groups or sub-groups'.

The purposes do not indicate that safe, scientifically robust, and ethical health-related research, *as a matter of principle*, would be an acceptable purpose for data disclosed to an ASH. Caldicott 2 added the new principle that 'the duty to share information can be as important as the duty to protect patient confidentiality'.[8] Our work on SHIP supports this, whereby a principled proportionate approach to governance is taken. SHIP's GGF makes clear that both adequate privacy protection and the undertaking of scientifically sound and ethically robust research are in the public interest. Moreover, what this means in practice is that those seeking to access, link, use or reuse data must "make the case" that the use will at least have a reasonable likelihood of furthering a particular public interest. The onus is on data custodians to demonstrate in what ways the public interest will be furthered.[9]

Furthermore, it is unclear whether the purposes delineating acceptable/permitted disclosures of data to an ASH reflect recent concerns regarding use of health data by, in particular, actuarial groups for health insurance purposes. The disclosure of health data to an ASH in order to analyse differences between population groups is precisely a type of activity that caused great public concern in relation to the care.data scheme.[10] In what concrete ways do the Regulations explicitly address the concerns that have been raised? Public engagement work indicates that individuals can recognise the public interests served by use of personal data for health-related research, whilst increased concerns are raised regarding access and use by commercial bodies.[11] Notwithstanding, our own work has indicated that commercial

[8] Department of Health, 'Information: To share or not to share? The Information Governance Review', March 2013, 21 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf> accessed 31 July 2014.

[9] Nayha Sethi and Graeme Laurie, 'Delivering proportionate governance in the era of eHealth: Making linkage and privacy work together' (2013) 13 Medical Law International 168–204.

[10] In a forthcoming article we consider how the care.data scheme failed to adequately provide a social licence for the proposed use of individual health data, highlighting the importance accounting and providing for the expectations of society regarding certain activities that may go beyond those formally required by law. Pam Carter, Graeme Laurie, Mary Dixon-Woods, 'The social licence for research: why care.data ran into trouble' (2014) (forthcoming).

[11] See for example: Nancy E Kass et al, 'The Use of Medical Records in Research: What do patients want?' (2003) 31 Journal of Law, Medicine & Ethics 429–433, 431-432; Margaret A Stone et al, 'Sharing Patient Data: Competing demands of privacy, trust and research in primary care' (2005) British Journal of General Practice 783-789, 786-787; Gill Haddow et al, 'Tackling Community

access is not necessarily a "no go" area for sections of the public, but there are serious objections when there is the prospect of "excess" or "obscene" profit.[12] However, commitments to share the benefits of access with the wider public or community – even if the access is by private entities – might help to assuage concerns. This is something that should be considered and accounted for at the drafting stage of the Regulations. We support access and use controls that focus on the public value and subsequent accessibility of benefits arising from data use, rather than whether the applicant comes from the "private" or "public" sector. This is an unhelpful and difficult distinction to draw. The maximisation of public benefit should be the driver.

Finally, whilst the proposed Regulations acknowledge the recommendation of using accredited safe havens as set out in the 2013 Caldicott Review, the narrow list of purposes provided does not reflect another core message of the same review, namely - the principle that '[t]he duty to share information can be as important as the duty to protect patient confidentiality.'[13] The revised Caldicott principles should play an integral role in the formulation of the Regulations. The limited purposes to which data may be disclosed to an ASH, and in particular, the lack of a purpose that would legitimise disclosure for safe and ethical research should be reconsidered prior to implementation.

Controls

Q2. Are there any other regulatory controls that you think should be imposed?

A principled proportionate approach to governance offers controls that both protect and promote the safe and ethical use of data. The twin public interests at stake are the appropriate protection of citizen privacy and other interests (clearly, a public interest in its own right), and the public interest of promoting scientifically sound research for wider public benefit. Crucial to achieving *proportionate* governance is an assessment of *both* risks and benefits associated with any proposed use of data. The list of controls to be imposed by the Regulations solely focus on the *protection* of

---

Concerns about Commercialisation and Genetic Research: A modest interdisciplinary proposal' (2007) 64 Social Science and Medicine 272–282, 275-276; Davidson et al 'Public Acceptability of Data Sharing Between the Public, Private and Third Sectors for Research Purposes' 63; Office for National Statistics, 'Beyond 2011 Public Attitudes Research: Report on 2010 Focus Group Research', 2014 7-8 <http://www.ons.gov.uk/ons/about-ons/who-ons-are/programmes-and-projects/beyond-2011/reports-and-publications/research-reports/index.html> accessed 17 July 2014; Office for National Statistics, 'Beyond 2011 Public Attitudes Research: Report on 2012 Focus Group Research', 2014 20-21 <http://www.ons.gov.uk/ons/about-ons/who-ons-are/programmes-and-projects/beyond-2011/reports-and-publications/research-reports/index.html> accessed 17 July 2014.

[12] Haddow et al, 'Tackling Community Concerns'.

[13] Department of Health, 'Information: To share or not to share? The Information Governance Review' 21 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf> accessed 23 July 2014.

data, without corresponding attention to the aim of facilitating safe and ethical use of data disclosed to an ASH.

Whilst governance of data flowing in and out of an ASH should be robust - technical fixes do not provide *complete* good governance, and importantly these cannot abdicate responsibility or supplant sound ethical decision-making about whether and how linkage, use and reuse of data should occur. Technical measures – such as adequate anonymisation – address the imperative that data use be *safe*. They do nothing to address whether the access is scientifically sound, or ethically robust. For example, might the research findings lead to increased discrimination or stigmatisation? Equally, while technical measures might reduce risks, such as re-idenitification, they do nothing to tell us about whether some degrees of risk are worth running because of the likelihood of considerable public benefits. Therefore, the controls imposed on data flowing in and out of an ASH should be clearly in proportion to the risks and benefits of specific data transactions. Proportionate yet robust governance can achieve the promotion of the full range of public interests at stake, including the protection of the data and individuals' privacy whilst also promoting publicly beneficial uses of the data such as for research in the public interest.

Our research on the SHIP initiative concluded that no single governance model is suitable for all circumstances. Numerous governance tools can, and should, be used – alone or in combination – to achieve an optimal approach in any given context. In particular, the three governance tools of anonymisation, authorisation, and consent should be considered for their relative benefits and limits. Thus, while anonymisation is largely a technical security measure, consent is an ethical device to support individuals to give expression to their autonomy. However, whether consent is necessarily the right governance tool relative to the risks and likely benefits at stake must be considered on a case-by-case basis. It is important to reflect, for example, whether the promotion of individual autonomy is the principal ethical consideration when determining whether data should be linked for health-related research in the public interest.

Q3. What are your views on the maximum amount of the civil penalty that we should set for breach of the controls proposed above in relation to ASHs?

In light of previous criticisms of a 'lack of teeth' regarding ICO powers,[14] we recognise the value which the threat of sanctions can bring in deterring data breaches and mishandling.

[14] Data protection law in the UK (prior to 2010 and the introduction of monetary penalties up to £500,000) was often criticised for its lacking deterrent quality, with limited offences for breaching the

Breaches and any concomitant civil penalties should account for the difference in the *nature* of the likely breaches: for example, compare: *intentional/wilful* abuses versus *negligent*/*unintentional* breaches.[15] It may be possible to consider whether *intentional* or wilful abuses of the controls support grounds for higher penalties than the suggested £5,000, whilst negligent or otherwise unintentional breaches could result in a lower scale of fines or other corrective action.

To illustrate: recent work undertaken by the Mason Institute and colleagues in the Farr Institute – CIPHER on behalf of the Nuffield Council on Bioethics and the Wellcome Trust Expert Advisory Group on Data Access uncovered that a key cause of harmful uses of health and biomedical data was maladministration or wider systemic organisational failures in the safe and ethical handling of such data.[16] Thus, the focus on imposing civil penalties on the *individuals* directly involved with a data breach may not address the underlying cause perpetuating such breaches in the first place. As such, the penalty scheme set forth by the Regulations might be re-oriented to provide higher *organisational* penalties for severe and/or persistent breaches by particular data controllers, whilst also maintaining similarly higher-level fines for wilful/intentional abuses of data by particular individuals. It is also important to ensure that all organisations and all individuals at all levels within organisations clearly understand their ethical and legal responsibilities around handling data. A clearer understanding of key responsibilities is likely to reduce the number of unintentional breaches. This speaks to the crucial importance of adequate training in information governance. As an example, consider the online researcher information governance module that we developed as part of the SHIP initiative: http://www.law.ed.ac.uk/teaching/online_distance_learning/cpd_courses/ship_information_governance/course_overview.

DPA 1998 and limited capacity for the Information Commissioner and Director of Public Prosecution to enforce the Act in England and Wales.

[15] For example, consider the difference between violations of the DPA which attract criminal liability under Section 55 of the DPA. Such offences are prosecuted by the ICO and provide examples of what are considered wilful/intentional abuses of data. Examples may be found on the ICO website: ICO Prosecutions <http://ico.org.uk/enforcement/prosecutions> accessed 31 July 2014.

[16] This report was jointly funded by the Nuffield Council on Bioethics, Wellcome Trust, Medical Research Council, Cancer Research UK and Economic and Social Research Council. Graeme Laurie, Kerina Jones, Chris Dobbs and Leslie Stevens, 'A Review of Evidence Relating to Harm Resulting from Uses of Health and Biomedical Data - Prepared for the Nuffield Council on Bioethics Working Party on Biological and Health Data and the Wellcome Trust's Expert Advisory Group on Data Access' (2014) (forthcoming).

Who might become an ASH?

Q4. Should there be any restrictions as to the type of body which might become (in whole or in part) an ASH, for example, a social enterprise, a private sector body or a commercial provider (working under a data processor contract)? Please let us know what you think.

We suggest that a public/private distinction between bodies seeking to become an ASH is unhelpful. Rather, the focus should be on the particular institution's ability to meet the standards for accreditation as an ASH. As we argue above, the overall public benefit to be delivered, should the body become an ASH, should be the guiding consideration, coupled with appropriate privacy protection. The character of the applicant should not, automatically, exclude them from being able to make a case that they can meet the standards for sound scientific and ethically robust research in the public interest. This having been said, it is clear after recent displays of public concern over care.data that meaningful exercises in public engagement are necessary above and beyond current efforts. A key finding of recent public engagement work undertaken by the Mason Institute suggests that publics do not make a straight-forward distinction between public and private data use. Public anxieties are increased when data are used to make *excessive* profit rather than there being *general* anxiety over data use by a particular type of organisation, public or private.[17]

Case management

Q6. What are your views on the level of the civil penalty that we should set for providers who do not comply with this duty?

Q7. Do you agree with the circumstances in which commissioners (case managers) should be able to obtain confidential patient information of an individual for whom they commission care?

Q8. What controls do you think should be in place in respect of such access? Please provide details.

In line with our response to question 3, the risk of civil penalties for non-compliance can serve an important deterrent function. However, a compromise position might be considered where a provider does not comply with the duty to share information from an individual's care record on the basis of that individual's *refusal* to the sharing (and that individual's refusal has not been legitimately overridden). In line with proposed

[17] Sarah Davidson et al, 'Public Acceptability of Data Sharing Between the Public, Private and Third Sectors for Research Purposes' 79.

ASH obligations to respect individual objections to processing, similar respect must be shown to individuals in relation to their care records. As suggested in para 48 of the Consultation, separate exploration into proposals for independent scrutiny and oversight of the receipt, acknowledgment and/or overall handling of individuals' objections is welcome.

We also hold concerns regarding the provisions for not seeking consent from, and/or overriding refusals by 'vulnerable' individuals receiving care; this seems to refer to individuals detained in a care setting (e.g. prison or secure mental health unit), and individuals referred to and starting to receive specialised mental health care services or admitted for treatment under the Mental Health Act.

Such provisions would grant disproportionate power to override the autonomy of the individuals implicated. We consider there to be clear differences between various vulnerable groups – vulnerabilities due to contextual setting (e.g. prisoners) or due to lack of capacity. Such differences should be reflected within provisions seeking to override individual autonomy. We are very concerned by the potential creation of a new category of "vulnerable" persons, which is insufficiently grounded in law. While the mental health legislation is concerned with persons affected by mental disorder, for the most part it only authorises treatment of the said disorder. In contrast, mental capacity legislation re-enforces the point that the starting presumption in law is that all persons have capacity, unless incapacity can be established. Even then, the law in question is on authorised treatment in the persons' own best interests (in England and Wales). The language of "vulnerable persons" is vague, ill-considered and potentially paternalistic. Its legal basis is questionable. We strongly urge the Department of Health to reflect on this terminology. While it might have resonance with emerging case law from the High Court with respect to its inherent jurisdiction, this has been the subject of considerable criticism.[18]

It is concerning that mental capacity is not mentioned. It is unclear how the suggested provisions would interact with current (and settled) legal determinations of mental incapacity under the Mental Capacity Act 2005. Determinations seeking to override an individual's autonomy should be considered on the basis of whether that individual can understand the particular issue they are being asked to make a decision about. We suggest the removal of allusion to efforts in favour of overriding such decisions from the Regulations.[19]

[18] See Barbara Hewson, 'Neither midwives nor rainmakers: why DL is wrong' (2013) Public Law 451-459; Caroline Bridge, 'Inherent jurisdiction' (2012) 42(Dec) Family Law Journal 1454-1456 and Ruth Hughes, 'The inherent jurisdiction over vulnerable adults' (2013) 3 Private Client Business 132-139.

[19] It is worthwhile noting current challenges against mental capacity legislation (e.g. the Mental Capacity Act 2005) especially in relation to involuntary treatment and potential inconsistency with the UN Convention on the Rights of Persons with Disabilities. For example see: Peter Bartlett, 'The United Nations Convention on the Rights of Persons with Disabilities and the future of mental health law' (2009) 8 Psychiatry; George Szmukler, Rowena Daw, and Felicity Callard, 'Mental health law and the UN Convention on the rights of persons with disabilities' (2014) 37 International Journal of Law and Psychiatry 245–252.

Controlling the release of data

Q9. What are your views of the controls set out above?

Q10. What are your views on the level of the civil penalty that we should set for any breach of these controls?

Q11. Are there any other controls that you think should be imposed? If so, please set out what you think these should be.

Robust data sharing agreements will play a crucial role in communicating to data recipients the terms and conditions of data use, including technical and organisational standards which must be met. It is surprising that use of data sharing agreements are not explicitly mentioned within the provisions, given their pre-eminence in existing best practices for data sharing.[20] Data sharing agreements can provide assurances of how data uses will be governed, regardless of whether or not the data are considered personal data.

Para 56 of the Consultation gives rise to some confusion and we would recommend revision and clarification of the point being made therein. Para 56 states that any information released from ASH would not constitute *personal* data 'because the controls would mean that they would not be able to link it to particular individuals, and nor would they be likely to get hold of information which would enable them to do so'. Despite this, it is held that the DPA 1998 would still apply to such transactions, despite the fact that the data would not constitute personal data (meaning the DPA 1998 does ***not*** in fact apply). It might be that the DPA 1998 would apply where a data recipient did seek to re-identify and link data to particular individuals (and was successful in doing so); however such obligations would not apply where the data held remained anonymous for the purposes of the Act.

[20] See for example the deployment of data sharing agreements under the SHIP initiative's Good Governance Framework and the recommendation by the ICO in its data sharing code of practice: 'Use SHIP to provide data access' <http://www.scot-ship-toolkit.org.uk/route-maps/custodians-assessing-requests-for-data/using-SHIP> accessed 23 July 2014; ICO, 'Data sharing code of practice' (2011) 26 <https://ico.org.uk/Global/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx> accessed 23 July 2014.

Equality issues

Q12. Do you think any of the proposals set out in this consultation document could have equality impacts for affected persons who share a protected characteristic, as described above?

Q13. Do you have any views on the proposals in relation to the Secretary of State for Health's duty in relation to reducing health inequalities? If so, please tell us about them.

Aside from the potential *positive* impact the Regulations might have upon the care of individuals, we contend that equally, there are potential *negative* impacts that might befall those individuals *deemed* vulnerable for the purposes of these Regulations (where such individuals may necessarily lack capacity to make decisions relating to the release of their care records or are perceived to be vulnerable because of their circumstances). The imposition of the potentially arbitrary label of "vulnerable" upon individuals *without* a protected characteristic under the Equality Act 2010 and *without* issues of capacity under the Mental Capacity Act 2005, may in fact lead to the discrimination of such individuals in contravention of the Equality Act 2010. We urge the Department of Health to consider the use and implication of the term "vulnerable" in general.

The response has been prepared for, and on behalf of, the Mason Institute Executive by:

Professor Graeme Laurie

Nayha Sethi

Leslie Stevens