Digital Economy Bill: Part 5, Chapter 1, clause 30 and Part 5, Chapter 2 from a health data perspective

medConfidential asks you to:

- **Express support for Baroness Findlay's amendment on Part 5 (NC213A-D)**
- **Express support for either amendment to Part 5 Chapter 2 (Clause 39)**
- **Oppose current Part 5 Clause 30 in Committee and on Report.**

The Delegated Powers and Regulatory Reform Committee has noted that clause 30 deliberately "excludes Parliamentary scrutiny" (para 37). We note that clause 30 does not amend the Data Protection Act. Departments will still only be able to do what they currently do. This being the case, removing clause 30 would not affect what Departments are currently able to do, with transparency; removing clause 30 will avoid greater secrecy in the way government uses data on classes of citizens for routine Departmental operations.

In 2009, the then Government removed clause 30's direct predecessor – clause 152 of the Coroners and Justice Bill – because the single safeguard offered then was ineffective. **This Government has not only excluded important aspects of Parliamentary scrutiny, it is trying to introduce "almost untrammeled powers" (para 21), that would "*very* significantly broaden the scope for the sharing of information" (para 4) without transparency, and with barely any accountability.**

Despite assurances, if the purposes of these powers can include, as per clause 30 (10)(a), individuals' "physical and mental health and emotional well-being", then health data must fall within the remit of this clause, whether it is held by the NHS or other bodies – such as schools, for example. medConfidential was led to believe that the Government was going to resolve this at earlier stages of the Bill – it has not – and it appears that decision may have come from the top of the Government Digital Service, whose stated priority is:

> *"the data-related work will be part of wider reforms set out in the Digital Economy Bill. [GDS Director General Kevin] Cunnington said as an example, that* ***both DWP and the NHS have large databases of citizen records, and that "we really need to be able to match those".*** *(interview)*

So, while there is a broad prohibition on the use of data from health and social care for research further down on the face of this Bill, in Chapter 5, the approach taken in clause 30 is very different, and contains no such prohibition. Regulations (currently draft) published under clause 36 simply omit the Secretary of State for Health from the list of Ministers, thereby excluding NHS bodies but not health data held by others. Quite aside from the fact that **the Secretary of State for Health could be added to regulations at any point, this is another fatal flaw in clause 30.**

To illustrate: when DWP forces a "customer" to reveal health data, and compels them to require the NHS to provide it, that data can then be copied onward to others at the whim of

the DWP, which has now become the data controller. Health information is no longer excluded from the powers of clause 30 as it no longer held by a body omitted from the regulations under clause 36.

DWP policy choices repeatedly demonstrate that it does not trust NHS assessments, yet it insists on acquiring more and more data from an institution the public trusts but it does not - the NHS. Clause 30 and the convoluted approach taken to supposedly 'excluding' health data from its effects will make such flows of data even more risky, deeply confusing for citizens as they will not know where their data may end up – further undermining public trust.

While the Fraud and Debt, and the Research and Statistics powers described in the Codes of Practice required by clause 36 provide for partial accountability, the Public Service Delivery powers defined in clause 30 – the single clause that affects most Departments – have significantly reduced oversight and, effectively, no transparency. We echo the deep concern of the Delegated Powers and Regulatory Reform Committee at these "inappropriately wide" powers (para 23) with utterly insufficient safeguards.

Public concern has recently been raised by Home Office demands for NHS Digital to hand over confidential patient data. The Home Office belief that any data should be made available if it serves a public policy requirement, while not unique, has been expressed on a number of occasions:

> *"How dare you even question our right to this information. This is data that belongs to the public. It is paid for by the taxpayer. We should use it for public policy."* - HSJ, 1/2/17

> *"**Mrs May**: I think what we are talking about is an attempt to ensure that we have access to information that is used in dealing with crimes that are taking place. If you are saying to me that you think there is certain information that should never be available to be used in terms of dealing with crime, I have to say I take a different view."* - Q78, Home Affairs Committee, Oral evidence: The work of the Home Secretary, 14/7/14

This is just one reason why transparency is so vital. In a meeting room on Marsham Street, the Home Office demands data from Departments while insisting on secrecy, and as paragraph 19.1 of the Home Office-DH-NHS Digital Memorandum of Understanding reveals, it even tried this with the NHS. The pretence of crime has been dropped in that Memorandum, as that MoU is purely about hunting for immigrants.

A policy-focussed civil servant argues that any data that may be useful to them should be available. Where does the line get drawn? How are competing interests balanced and what is the evidence base for that debate?

Just as a citizen should know how taxpayers' money has been spent, they should be able to see how their data is used. Just as the public sector publishes spending information, it should publish agreements to copy citizen data and why.

For patient confidence, for public confidence, there must be transparency over every agreement to share data under this legislation. Baroness Finlay's amendments would provide this (NC213A-D).

Chapter 2

medConfidential is deeply concerned that Chapter 2 of Part 5 contains no safeguards against bulk copying of civil registration data. We accept the case for a power to disclose civil registration information *on an individual consented basis* – a citizen should be able to choose to let the registrar inform other bodies of changes – but, just as clause 30 contains insufficient safeguards and is designed to enable bulk copying, so is Chapter 2.

The new section 19AA (5), added by clause 39 (2), removes any limit to copying registration data in bulk when it could instead provide for individual consent.

The Registrar General wishes an explicit legal basis for release of information to other Departments with an individual's consent, but clause 39 as drafted also provides the power to release bulk registration data on the entire population, without consent and – as the Delegated Powers and Regulatory Reform Committee has noted (para 52) – without even allowing for Parliamentary scrutiny. This power is as "inappropriately wide" as those in clause 30, and deliberately so.

medConfidential

coordinator@medConfidential.org