Data Protection Bill
House of Commons, Report Stage
Wednesday 9th May

About the BMA
The BMA is a professional association and trade union representing and negotiating on behalf of all doctors and medical students in the UK. It is a leading voice advocating for outstanding health care and a healthy population. It is an association providing members with excellent individual services and support throughout their lives.

Key points: safeguarding medical confidentiality

- **New Clause 12**: the BMA has been vocal in its opposition to an MoU (memorandum of understanding) between NHS Digital, the Home Office and the Department of Health and Social Care.¹ We – and many others² – believe it falls short of the well-established ethical, professional and legal standards for confidentiality.

NC12 would clarify that confidential patient data (including names and addresses) can only be disclosed by NHS Digital and other health bodies, in connection with the investigation of criminal offences, if the offence under investigation can be defined as a ‘serious offence’. This high threshold for breaching patient confidentiality is a principle which is well-established under common law, but is being disregarded by signatories of the MoU.

We urge MPs to support NC12 to ensure that only a ‘serious offence’ warrants a disclosure, aligning statute with the common law.

- **Clause 16**: the BMA has repeatedly expressed its concern that clause 16 would give the Government an inappropriate power to change the law, without adequate scrutiny or oversight via secondary legislation, on how confidential health data are shared. If this is not the Government’s intention, it should be reflected in the Bill.

We urge MPs to safeguard the Bill so that any changes to the application of the GDPR (via regulations amending this Bill) would not set aside the protection for patients in the common law regarding their confidential data.

**New Clause 12**

*Background*
Confidentiality is essential for the preservation of trust between doctors and patients – it is what reassures patients to be frank with their doctor, often confiding very personal, medical and non-medical information about themselves, safe in the knowledge that the doctor is under a duty not

---


to share the information (save in truly exceptional circumstances, as defined by the General Medical Council and the common law).

If patients feel they are unable to be frank with their doctor it makes it impossible for the doctor to provide fully effective treatment – or patients may simply not visit their doctor at all. A breakdown in trust is not only a danger to that individual’s health, but could also pose a serious threat to the wider wellbeing of the public if infectious diseases are either not identified and treated, or are diagnosed and treated at a later stage.

The BMA and a number of authoritative stakeholders have been extremely concerned by the discovery that NHS Digital has been risking this relationship between doctor and patient without due regard to the public interest in a confidential health service. NHS Digital has been routinely disclosing confidential patient information (name and address) to the Home Office, where people are suspected of committing an immigration offence.

We believe it is entirely inappropriate that NHS Digital – the “guardians of patient data”3 – is continuing to share data, knowingly, in a manner that is incompatible with the common law duty of confidentiality, as well as the key professional guidance on confidentiality4 (including even its own code of practice).

As highlighted by the Health and Social Care Select Committee, data provided by patients for health and care purposes should only be shared for law enforcement purposes in the case of ‘serious crimes’ – it has been repeatedly pointed out to NHS Digital that most cases of immigration enforcement will not meet this high threshold for disclosure.

**BMA position: support for New Clause 12**

Despite overwhelming condemnation of the MoU, NHS Digital and the Government have refused to take a more balanced approach and properly consider the public interest in maintaining a confidential health service weighed against disclosures in the public interest. Their justification has been that the practice outlined in the MoU is lawful, under a legal gateway in the HSCA (Health and Social Care Act).

However, although this legal gateway is a necessary requirement for such disclosures it is, crucially, not sufficient in isolation. The National Data Guardian has been clear that disclosures of confidential information must also be justified under the common law, which sets a higher bar: “the different requirements of the statute and the common law are not unhelpful inconsistencies to be solved or removed, but rather two standards, both of which must be satisfied”.5

NC12 would ensure that this higher threshold is enforced by aligning statute with the common law. It would clarify that confidential patient data (including names and addresses) can only be disclosed by NHS Digital, in connection with the investigation of criminal offences, if the offence under investigation can be defined as a ‘serious offence’. We believe this would lead the signatories of the MoU to reevaluate the approach that they are taking when making judgements about disclosures ‘in the public interest’.

**We urge MPs to support NC12 to ensure that the existing legal and ethical duties to protect patients’ personal information from improper disclosure are enforced, and trust in the doctor-patient relationship is maintained.**

---

4 GMC guidance states that information can be disclosed ‘to protect individuals or society from risks of serious harm, such as serious communicable diseases’ or when it is necessary ‘for the prevention, detection or prosecution of serious crime’. Online at: https://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp
Clause 16

Background

Clause 16 embeds a provision in Article 6 of the GDPR for member states to determine “specific provisions to adopt the application of the [GDPR] rules” regarding lawful data-sharing. Rather than setting out these “specific requirements” on the face of the Bill, clause 16 legislates for the UK Government to define its adaptation of the GDPR in subsequent secondary legislation – to be made by the relevant Secretary of State and affirmed by Parliament (the ‘affirmative resolution’).

As a result of this clause, parliamentarians are being asked to give the Government extremely wide powers to make future changes to the rules on sharing of confidential data (potentially including health data) without any specifics as to how this power will be used or what, if any, restrictions will be applied.

Attempts\(^6\) in the Lords to address this point, by increasing the level of scrutiny of future regulations to the more rigorous ‘super affirmative’ procedure, were denied. Moreover, warnings from two expert House of Lords select committees\(^7\) were disregarded: the committees reported on the worrying scope of the regulation-making power in clause 16, calling attention to the “insufficient and unconvincing” justification\(^8\) provided for its inclusion in the Bill, and recommending its “removal from the Bill”.

BMA position: opposition to clause 16

The BMA has consistently raised its concern about the specific impact that the scope of clause 16(1)(a)’s regulation-making power could have on medical confidentiality – allowing the Government to override the common law duty of medical confidentiality, should it choose to do so.

In response to probing amendments, ministers recognised that further work was needed to balance future-proofing the Bill with ensuring proper parliamentary scrutiny of subsequent delegated powers. Importantly, Lord Ashton gave a specific “reassurance”, in response to a probing amendment, to consider the clause’s potential impact on confidential patient data: “the Government are committed to looking at the issue of delegated powers in the round. I will certainly include that [amendment 108A] in that discussion”.

The BMA has not been reassured by the Government’s subsequent revisions to the Bill, which have not altered the provisions in clause 16(1)(a). Our understanding remains that the Bill allows the Government to make regulations in the future that could alter the application of the GDPR without thorough oversight or consultation – including the power to alter data-sharing arrangements concerning confidential health data.

At this final stage of the Bill’s scrutiny, the BMA urges the Government to act on the select committees’ expert advice and concerns expressed in Parliament. We do not believe the new regulation-making power in clause 16 is fit for purpose, and urge MPs to remove the remaining uncertainty about 16(1)(a)’s scope and application on the face of the Bill.

May 2018

For further information, please contact:
Holly Weldin, Senior Public Affairs Officer
T: 0207 383 6515 | E hweldin@bma.org.uk

---

\(^6\) Amendments were proposed by Lord Clement-Jones, Lord Paddick, Baroness Jones, Baroness Neville-Rolfe and Lord Arbuthnot.


\(^8\) Baroness Williams, Minister of State at the Home Office, Second Reading of the Data Protection Bill: “Given how quickly technology evolves and the use of data can change, there may be occasions when it is necessary to act relatively quickly to provide organisations with a legal basis for a particular processing operation.”