Question 1: Please tell us which group you belong to? (Required)

British Medical Association

Question 2: If you are a member of an organisation or profession, please tell us if you are responding in a personal or private capacity

N/A

Question 3: If the Department of Health or other organisations were to create further opportunities to engage on data security and the consent/opt-out model, would you be interested in attending? If so where would you find it helpful an event to be held?

• Yes • No

Event location

Preference for London but would make efforts to attend any location.

Question 4: The Review proposes ten data security standards relating to Leadership, People, Processes and Technology. Please provide your views about these standards.

Which standard do you wish to comment on?

1 2 3 4 5 6 7 8 9 10

Comments

We strongly support all ten standards which are a helpful and concise illustration of organisations’ responsibilities. We are pleased that the standards will apply to all organisations which handle health and social care information.

In relation to standard two, we know that health care organisations have been the subject of criticism from the Information Commissioner over the number of data breaches or losses. In many cases the breaches are as a result of poor information governance practice rather than technical failures. Raising awareness of the importance of good information governance is essential and educating people on how to handle and store data appropriately will go a long way to ensuring its security. Promoting a culture of good practice in data protection within an organisation is paramount given that human behaviour is the key to keeping confidential information secure.
Aside from the standards, we also believe that in the same way in which clinical errors should be treated as an opportunity to learn rather than an occasion to identify a scapegoat to punish, information governance failures such as an accidental data breach should be addressed likewise. This could involve a ‘significant incident’ style investigation to identify root causes and make recommendations for changes to prevent mistakes happening again. A good example of this practice is the way in which Chelsea and Westminster Hospital NHS Foundation Trust dealt with the accidental disclosure of the email addresses of individuals who subscribed to an HIV service in 2015. In this case, the response of the Trust included a systematic review of the incident and changes being made to how email is managed to avoid a reoccurrence of the breach.

Question 5: If applicable, how far does your organisation already meet the requirements of the ten standards?
Where 0 = Not at all and 10 = Fully compliant

0 1 2 3 4 5 6 7 8 9 10

Please provide examples which might be shared as best practice

N/A

Question 6: By reference to each of the proposed standards, please can you identify any specific or general barriers to implementation of the proposed standards?

Which standard do you wish to comment on?

1 2 3 4 5 6 7 8 9 10

The NHS is experiencing intense financial and workload pressures, directly caused by continued underinvestment and overly burdensome regulatory requirements. Significant and ongoing investment across all three themes of people, process and technology will be required to enable healthcare organisations to implement and maintain compliance with the proposed data security standards. Without new investment, the standards risk creating even more burden for smaller healthcare organisations, such as general practices.

Such investment would include funding for people to dedicate time and resources within their organisations to ensure that information governance, and the training that supports good practice, is given a high profile so that staff understand its importance. For some organisations this may require a cultural change so that the importance of information governance is recognised at a senior level and that training is not seen as a one-off ‘tick box’ exercise, but a continuous process.

The key issue is to ensure that staff are able to understand, and recognise the importance of, the basic principles in line with their role and are therefore adequately prepared to apply their knowledge to different scenarios in their daily working routines. We recognise that this may not always be easy due to the complex nature of information governance and therefore it is important
that there are prominent people within each organisation available to provide support and advice if there is uncertainty about how to manage data in the appropriate way.

Organisations should have formal mechanisms in place to ensure every member of staff is up to date with appropriate training on information governance and data protection. Staff should also receive training on how to use IT systems in general, to avoid accidental misuse that increases risk of data security breaches. This should include those who work on a temporary basis such as locums and doctors who are on rotation. These staff are frequently placed in difficult positions, for example, having to ‘borrow’ a colleagues’ password as the organisation has not issued them with their own log-in details and where patients may be at risk of harm if information is not accessed.

Annual and comprehensive training for all staff will require significant financial investment from healthcare organisations if it is to be more than a ‘tick box’ exercise. The nature of training can be shaped according to the needs of each organisation, for example, it would be more appropriate for general practice staff to participate in in-house training sessions, rather than being expected to attend formal courses individually, which can be costly and require significant time out of the office.

Healthcare professionals need to have functional hardware and software that enables them to maintain data security while continuing to deliver clinical care. To do this, there needs to be increased and sustained investment in NHS IT by DH, Health and Social Care Information Centre (HSCIC) and NHS England, which enables programmes of regularly updating software and hardware. The BMA echoes concerns identified by the NDG review that policies and processes need to be designed to support the needs of staff to avoid workarounds and data security breaches. One clear example where processes inhibit staff to do their job is the lack of rapid, assured single sign on software in many healthcare organisations. Where organisations do not have funding for this, additional funding should be provided by relevant bodies. For example, within general practice, all new systems should be deployed via the GP Systems of Choice (GPSoC) programme or an equivalent.

In addition, healthcare professionals require timely access to general IT help and support to resolve technical issues in a timely manner. Relevant bodies should ensure there are adequate dedicated resources made available to provide technical support for IT systems, either through contracts with suppliers and/or a dedicated help support service.

**Question 7: Please describe any particular challenges that organisations which provide social care or other services might face in implementing the ten standards.**

It is very important that resources are provided to ensure appropriate training for all staff who handle data so that local authority culture is transformed to reflect the same standards of confidentiality which exist in the NHS.

The key challenge will be the impact on social care staff and resources, to introduce secure IT and train staff to use it, many of whom might be more unfamiliar with IT systems and records. Funding and capacity in this sector is already very strained, so this expectation could push it past its limits of safety and care quality.

**Question 8: Is there an appropriate focus on data security, including at senior levels, within your organisation?**

- [ ] Yes  - [ ] No

Please provide comments to support your answer and/or suggest areas for improvement
Question 9: What support from the Department of Health, the Health & Social Care Information Centre, or NHS England would you find helpful in implementing the ten standards?

As stated above, health and social care organisations will need to provide sustained financial and human resource investment to implement and maintain compliance with the data security standards. This will include initial additional investment in change management, to change workplace cultures to be more data security focused, as well as investing in appropriate technology such as single sign on software. There will also be ongoing resource implications for maintaining up to date hardware and software, monitoring and reviewing data security in line with the standards, and providing comprehensive ongoing training. The DH, HSCIC and NHSE could support this work to be successful by providing additional funding for this work.

The BMA welcomes standard eight, which proposes that no unsupported operating systems, software or internet browsers are used within the NHS IT estate. The BMA recommends, however, that close consideration be given to the best way to ensure that the NHS is not placed at the mercy of software suppliers for meeting the cost of newer versions which will redirect significant resources away from patient care. Support would be needed from DH and HSCIC to ensure suppliers update software regularly to ensure health and care organisations can respond to a rapidly changing environment.

GPs are liable for ensuring that any data sharing they are engaged with complies with the Data Protection Act 1998 (DPA). Practices do not always have the expertise or the resources to negotiate local data sharing agreements, which can be highly technical and complex. To ensure that staff are equipped to understand how to handle information properly, and how to share information with CCGs, we urge NHS England to develop further national guidance on data sharing to help practices to determine the legal basis for sharing for local commissioning and healthcare purposes.

Question 10: Do you agree with the approaches to objective assurance that we have outlined in paragraphs 2.8 and 2.9 of this document?

☐ Yes  ☐ No

Please comment on your answer

Yes, but with a significant qualification.

We have serious concerns over entrusting the complexity of making judgments about an organisation’s security arrangements to the CQC.

We strongly support the GPSoC approach as this provides an assurance process which is managed between GP users, their representatives, the NHS and approved system suppliers. This process has provided sufficient assurance over twenty years. We strongly believe that the CQC’s involvement
in this area of general practice should be limited to confirming the practice’s adoption of these approved systems.

Fundamental changes would be required to the CQC’s current approach before the BMA could be confident that it is competent to provide a supportive approach which will help organisations deliver high standards. Training for CQC inspectors is paramount and should have representative GP input. The CQC should look to the model under Health Inspectorate Wales.

We are supportive of a revised and organisation specific IG toolkit and agree there should be a mechanism or risk assessment process to identify organisations which require further support so they can be helped to achieve high standards.

**Question 11: Do you have any comments or points of clarification about any of the eight elements of the model described above?**

*Which standard do you wish to comment on?*

- [ ] 1
- [ ] 2
- [ ] 3
- [ ] 4
- [ ] 5
- [ ] 6
- [ ] 7
- [ ] 8

Please provide details

The BMA supports all eight elements of the proposed model (with a significant qualification to standard four).

Our comments focus on standards four and seven.

**Standard four - ‘You have the right to opt-out’**

We support the right to opt-out, however, what is proposed is highly selective and potentially misleading.

The Review proposes that, where a legal basis exists, personal confidential data should be shared with the HSCIC (now NHS Digital), as the statutory safe haven, so that it can apply de-identification or anonymisation processes to the data to allow dissemination to organisations needing to use them. The right to opt-out therefore does not apply to:

i) flows of personal confidential data into the HSCIC under directions\(^1\) and;

ii) flows of data out from the HSCIC which are anonymised in-line with the Information Commissioner’s (ICO) anonymisation code of practice.

Whilst there can be no doubt about the extremely valuable work of the HSCIC in providing high quality linked data which can be used for the benefit of running the health service, removing the right for patients to prevent their confidential data from leaving the GP practice where the HSCIC is following statutory directions (the ‘Type 1’ objection) causes the BMA serious concerns. It is a removal of the reassurance given by the Secretary of State for Health in 2013 in relation to care.data and the powers under the Health and Social Care Act 2012 (HSCA).

It is a fundamental change if neither patients, nor GPs, have the ability to control the disclosure of confidential data to the HSCIC when directed by NHS England or a future Secretary of State for Health. If this concept is carried to its natural conclusion the HSCIC could hold a database of the medical records of every NHS patient. Patients are, therefore, being asked to place their trust in the HSCIC, rather than the traditional holder of their life-long medical record. This removal of the ability of patients to trust the medical profession to protect their information risks potential

---

\(^1\) I.e. Directions under the Health and Social Care Act 2012 s.254
catastrophic consequences. If patients fear that they cannot be honest with their doctor this will not only have serious consequences for their own healthcare but will also diminish the value and completeness of the data for secondary purposes. These concerns are not mitigated by the argument that it would be inconsistent to allow an opt-out for GP data to be shared with the HSCIC but not for hospital episode statistics (HES) data.

As the report recognises, the public place great trust in their GP. GPs have traditionally carried out the role of ‘record guardian’ for their patients – a role which, in our view, is fundamental to maintaining confidentiality and trust. Survey findings consistently demonstrate that GPs are seen as the most trustworthy guardians of health information.²

The question of trust is crucial in the current climate. This issue is rightly given prominence in the report. As a result of the 2014 public controversy over the care.data programme, past disseminations of HES by the HSCIC and subsequent Health Select Committee inquiries, public trust in ‘the system’ and, more specifically, the HSCIC is low. We recognise that the HSCIC has significantly strengthened its dissemination procedures and governance controls following the Partridge review³ and implementation of the Care Act 2014⁴, however, it seems highly optimistic that the public would be willing to trust the HSCIC so quickly after the events of 2014. In our view, the HSCIC would need to demonstrate a proven track record of data stewardship and in disseminating data appropriately and responsibly over a number of years before public (and professional) trust could be confidently relied upon to the extent that the right to opt-out can be removed.

The change in the name of the HSCIC to ‘NHS Digital’ on the grounds that it ‘will provide the organisation with a good opportunity to use the NHS brand making it clear to everyone that it is part of the NHS ‘family’ requires extremely careful handling. It is important that patients are aware of the benefits to the NHS through the use of data processed by the HSCIC, nevertheless, this change - in name only - could result in a situation where patients and the public feel they have been misled given that the HSCIC is not actually within the NHS. Unless the role and status of the HSCIC is made clear in future conversations with the public, the name change could result in a situation where it is perceived that confidential data are being shared within the ‘walled garden’ of the NHS as a disguise for a government data collection. In other words, there is a risk that any future national data collections from GP practices could be perceived as ‘care.data by another name – but without the opt-out’. Such perceptions must be avoided if irreparable damage to public trust is not to be done and if future national data collections, and the numerous benefits they may bring, are to be successful.

Public acceptance and trust in the HSCIC is unlikely to be gained by removing or limiting controls to share data with it, particularly given recent evidence which emphasises the importance to the public of the right to opt-out.⁵ In our view, consultation should be had with the public about the benefits and risks of data sharing with the HSCIC so that they can make a choice about the level of risk which is acceptable to them. Whilst we understand that the changes made to the HSCIC’s data governance framework following the Partridge review mean that the HSCIC employs high standards of security and has a robust framework for data dissemination which make the level of

---
² Medical Research Council and Ipsos MORI (2007) The Use of Personal Health Information in Medical Research General Public Consultation Final Report, p.45
³ Sir Nick Partridge (2014) Review of data releases by the NHS Information Centre
⁴ Care Act 2104 s122
⁵ Citizens’ jury events in 2016 concluded that patients should be notified of information sharing schemes and have the right to opt-out if they chose. The Citizens’ Juries (2016) Health Data on Trial http://www.herc.ac.uk/get-involved/citizens-jury/
risk minimal when compared with the benefits, nevertheless, risks do exist. The central storage of rich datasets in one place makes data a more attractive target for a malicious cyber-attack or it may encourage ‘mission creep’ amongst potential users of the data. A number of patients might be fearful of these risks, particularly given the rapid increase in the understanding of genomics and the potential increase in this information being held in the medical record. Or, some patients will simply be unhappy with an organisation other than their GP practice holding and controlling their clinical history. Equally, once they are aware of safeguards which are applied to data, the limiting circumstances under which they can be shared and are more informed about the way in which the NHS uses data and the associated benefits, many patients may not wish to exercise the Type 1 opt-out. One of the key problems which undermined confidence in the care.data programme was the confusion around what the data would be used for once it was inside the HSCIC and the perception that it could be sold to commercial companies outside of the NHS. The crucial point is that patients should be able to make an informed choice based on clarity of information and transparency. An additional step towards improving transparency could be the development of a central register where individuals can check what opt-out choices they have made in the past (at both GP practice level and at HSCIC) and how their data have been used.

The review is silent on the question of whether the identifiers which will flow into the HSCIC under the statutory directions will be destroyed following the linking and pseudonymisation processes. Should the identifiers be retained this will potentially allow for re-identification in the future therefore the governance arrangements for holding the identifiers, and the controls around the potential reversal of the pseudonymisation, are crucial. We recognise that there are certain occasions when it will be necessary to re-identify individuals following linkage, for example risk stratification, therefore the forthcoming engagement work with the public must be clear how identifiers are protected and under what circumstances they can be accessed.

One of the arguments for removing the ‘Type 1’ opt-out is to ensure complete datasets but we are not convinced of the necessity for complete datasets. There are very few research projects or commissioning needs that require a complete dataset and, where access to a complete cohort is required, this could be managed through application to the Confidentiality Advisory Group using regulations under s251 of the NHS Act 2006. This would allow each requirement to be independently assessed according to its merits. The argument that by having a complete cohort of pseudonymised datasets, researchers and commissioners would no longer require identifiable data is weak and appears to be based on convenience and speculation rather than evidence. A convincing evidence-based case would be required before the BMA could support this approach.

It is certainly not our intention to appear to be overly critical of the HSCIC. We have previously been supportive of its role as the statutory safe haven as a way of providing increased regulation and control of data flows, and importantly, as the mechanism by which multiple local data flows of questionable legal basis can be avoided. Our comments reflect our concerns that, in the desire to collect and realise the benefits of data, removal of patients’ choice and control will ultimately have the opposite effect through the loss of trust. In our view, this is not a risk which is worth taking without the clear agreement of the public. The issues we have outlined here must be squarely confronted with them. Our position is that both the ‘Type 1’ and ‘Type 2’\(^6\) opt-out choice must remain for all patients unless the public clearly indicate otherwise.

\(^6\) Opt-out of personal confidential data leaving the HSCIC (for reasons other than direct care).
Standard seven – ‘The opt-out will not apply to anonymised information’

We support the concept of data which are ‘de-identified for limited access’ or anonymised in context so that it can be disseminated by the HSCIC to allow the majority of commissioning and research to take place safely with minimal risk to confidentiality.

Provided patients can exercise the ‘Type 1’ opt-out, we agree that the ‘Type 2’ opt-out should not apply to data which are anonymised in context as this provides a practical and reasonable solution to make use of data for health benefit purposes. We would, however, welcome further clarification about this category of data as described in the ICO’s anonymisation code of practice.\(^7\) We understand that these data are person-level data, subject to contractual controls and stewardship arrangements which prohibit re-identification, however, it would be helpful to more clearly understand whether all, or some, identifiers need to be removed before it can be considered to be de-identified for limited access according to the ICO code. Is the ICO definition of de-identified data for limited access analogous to the ‘de-identified data for limited’ access as described in Dame Fiona Caldicott’s 2013 information governance review and which contains a single identifier such as NHS Number?

Question 12: Do you support the recommendation that the Government should introduce stronger sanctions, including criminal penalties in the case of deliberate re-identification, to protect an individual’s anonymised data?

Yes. The BMA has long since held the view that there should be strict repercussions for deliberate misuse of confidential data. We would welcome the option of custodial penalties being imposed in serious cases and believe that such penalties would be a far more effective deterrent than the current fiscal sanctions.

We are aware that consideration has been given to the introduction of custodial penalties in the past and are disappointed that, despite the support of the Information Commissioner’s Office, the relevant provisions under section 55 of the DPA have not been enabled.

It is important to note that we are specifically focusing on introducing custodial penalties for those who deliberately and/or maliciously misuse confidential data. We are not advocating to penalise individuals who, for example, make a genuine mistake or an error of judgment in relation to a difficult decision as to whether to make a disclosure in the public interest.

Question 13: If you are working within health or social care, what support might your organisation require to implement this model, if applicable?

This question is aimed at health and social care bodies, however, BMA members stressed that time, training, resources and a clear curriculum are fundamental to successful implementation of this model. This includes the delivery of reliable and secure IT systems, including for those workers who move between sites or go to outlying clinics or make home visits, are fundamental. The need for healthcare staff to carry paperwork around with them should be removed.

---

\(^7\) Information Commissioner’s Office (2012) *Anonymisation: managing data protection risk code of practice*, chapter 7
Question 14: If you are a patient or service user, where would you look for advice before making a choice?

Members of the BMA’s Patient Liaison Group (PLG) were unclear where they would seek advice, with the default option being their local GP surgery. This reflects the current confusion for patients and the public about the important issues raised in the consultation.

Members of the PLG were not aware of the HSCIC and were concerned about their powers to hold patient data. Again, this underlines the significance of the public engagement work, and in particular, in explaining the role of the HSCIC.

Question 15: What are your views about how the transition from the existing objection regime to the new model can be achieved?

☐ Yes  ☐ No

Please comment on your answer

The BMA does not have any comments on this question.

Question 16: 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?

The BMA does not have any comments on this question.

Question 17: 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.

As discussed above, we support the principle of using data which are anonymised in context. The use of these data on a national scale can help to reduce health inequalities through the identification of those groups whose needs are not currently being met by the health service. It is crucial that the correct balance is struck between using data to reduce inequalities and drive improvements whilst not undermining confidentiality through removal of the right to opt-out.

Send your responses to: