



## Department of Health

### National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs

#### Response Form

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

Response on behalf of Professional Organisation: Royal College of Physicians of Edinburgh

**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

**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

The data security standards are welcomed. Most organisations already have mandatory training for all staff in Information Governance (IG) with the need for annual re- certification (standards 1-3).

There is a need for greater focus on cyber security as this is an area where threats are increasing but many health and care organisations have immature processes and systems in place to identify and manage risk (5,6,7,9). The national data guardian highlights the need to raise the profile of data security at Board level and for executive leadership to change culture.

Standards 4 and 8 are likely to be the most challenging to meet.

---

**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

RCPE Fellows are based at NHS Trusts around the country. Some NHS Trusts have recently created new posts in digital services which focus on data security. Examples include those who have processes for monitoring IG breaches which are good and involve regular reporting of all breaches to the Deputy CEO, who is the executive lead for digital and data security and who also acts as the Trust's Senior Information Risk Owner (SIRO).

In these circumstances, clinicians work closely with managed technical partners to ensure there is adequate monitoring of cyber threats and all incidents are reported immediately to senior management and in regular updates to the Board.

Fellows have reported that management of IT accounts for starters and leavers can be poor, and staff may use workaround solutions to access systems they need, often with inadequate training. Fellows are aware that in some NHS Trusts unsupported browsers are used, however generally these are now being updated.

**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

Standard 8: One of the constraints which has led people to continue to use unsupported operating systems or browsers is that clinical applications, including some of the national applications, only function on outdated versions. Unless IT suppliers and NHS Digital are mandated to ensure their applications work on modern operating systems and browsers it will not be possible for NHS organisations to meet this standard.

It may also be difficult for many NHS organisations to recruit or retain people with the necessary data security skills and expertise if services are managed in house.

---

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

The RCPE has no specific comments on this question.

**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

The RCPE has no specific comments on this question as our Fellows are based in many different NHS Trusts.

**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?**

Ensure all suppliers of clinical appliers and national systems developed by HSCIC are supported on the latest versions of operating systems and browsers.

**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: internal and external audit, supported by CQC review are welcomed.

**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 opt out model is still likely to be confusing for people. Patients are told they can ask for some components of their personal confidential information to be withheld from others involved with their care. Most digital clinical applications do not support sharing or withholding individual data components so this may not be achievable.

The proposal to share all personal identifiable data with HSCIC is likely to lead to resistance. Further clarification is required as to why this is necessary and whether patients who opt out can refuse to have their data send to HSCIC for de-identification.

It is unclear whether the new proposals are suggesting that HSCIC is the only safe haven that should

be holding personal identifiable data and what the plans are for existing accredited safe havens which hold personal identifiable data and whether section 251 exemptions will still be relevant in the future.

**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 public needs to be assured that their data is managed appropriately.

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

There are currently numerous different information sharing and consent models which have been implemented within local health and care economies. It would be helpful to have a national public engagement campaign and a confirmed process for opt out and consent which is then implemented consistently across the country.

As Sustainability and Transformation Plans (STPs) and local digital footprints are being asked to develop data sharing agreements and agree consent models for their own local health economies, national agreement and guidance is required sooner rather than later to avoid the need to repeat public consultation exercises. Systems to manage and share citizen consent should be implemented at either a national level or regional level.

**Question 14: If you are a patient or service user, where would you look for advice before making a choice?**

N/A

**Question 15: What are your views about what needs to be done to move from the current opt-out system to a new consent/opt-out model?**

Yes  No

Please comment on your answer

For the various reasons outlined above the transition to the new model will be difficult and requires the national bodies to proceed with a public engagement exercise sooner rather than later.

**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 RCPE has no specific 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.**

The RCPE has no specific comments on this question.

**Send your responses to:**

NDG's Review of Data Security, Consent and Opt-Outs  
Room 2N12  
Quarry House  
Quarry Hill  
Leeds  
West Yorkshire  
LS2 7UE