Response ID ANON-2BBS-3UZ2-W

Submitted to **New data security standards and opt-out models for health and social care**
Submitted on **2016-09-04 13:13:05**

Foreword

Introduction

1 Please tell us which group you belong to.

Group title:
Professional Organisation/Association

Other - Please specify:
EMIS National User Group: representing users of the largest of the principal GP electronic health record systems

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

Capacity in attending:

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

Event location:
Adequate notice is more important that location. London is generally accessible from all parts of the country.

Data Security

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? - Which standard do you wish to comment on?:
6

Comments:
Standard 3: It is important that the training and education material is of high quality, relevant to the user; and that any testing is not overly bureaucratic or time-consuming. It will be helpful to have consistent training material available in one place.
Standard 3: Can the standard be re-worded to “All access to personal confidential data on IT systems WILL be attributed to individuals” to avoid any ambiguity as to whether this actually happens or just needs to be possible.
Standard 6. In order for organisations to be able to respond to CareCERT security advice (http://digital.nhs.uk/carecert) , the advice needs to be timely and relevant to the organisation. It must be clear when this advice be available and how the cost implications will be met
Standard 8 (no ‘unsupported’ software): In order for this standard to be appropriate, there must be a clear definition of supported and unsupported software. It is important that responsible agencies do not withhold support for software without good reason and approve software in a timely manner. Failure to do this could result in a loss of business efficiency and a delay to new services.
Standard 9. The training and cost implications for general practices to meet the Cyber Essentials security framework need consideration https://www.gov.uk/government/publications/cyber-essentials-scheme-overview. We note that the “10 steps to Cyber Security” recommended in the overview has been withdrawn since 11 July 2016.
Standard 10 clarifications are needed as to who suppliers will contract with for protecting the personal confidential data they process on behalf of GP practices (who are data controllers). Will the contracts be between the practices and the suppliers or between the CCG and the suppliers or some other organisations?

5 If applicable, how far does your organisation already meet the requirements of the ten standards?

Standard Requirements - Where 0 = Not at all and 10 = Fully Compliant:

Please provide examples which might be shared as best practice:

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

Please provide your views about these standards.:
4. This standard will pose a significant challenge to large trusts, in many of which access to electronic systems (egg results) is not governed by access controls based on legitimate relationships. Once a patient is on the hospital system all staff at a level having access have access to all results egg a sister on the gynaecology unit can view the results of a patient under the care of a dermatologist. Resolving this will require major organisational as well as technological change. Clarification is needed regarding which organisation is responsible for holding contracts with suppliers within the GP practice setting. Is it each individual practice (as data controller) that needs to have a contract with the supplier (data processor) or the CCG on behalf of practices in which case does each practice need to have this built into a contract with the CCG? There could be considerable cost implications of implementing the security standards. Clarification on how

these costs will be met is needed and also how often will these requirements change

Which standard do you wish to comment on? - Which standard do you wish to comment on?:
4

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

Please provide your views about these standards.:

8 Is there an appropriate focus on data security, including at senior levels, within your organisation? Please provide comments to support your answer and/or suggest areas for improvement.

Not Answered

Please comment on your answer:

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?

Please provide your views about these standards.:
The greatest need will be for educational programmes and business process change management. This will be required to develop understanding of who does need access to information (who has a legitimate relationship) and how to create staffing and structural models that support these relationships. Within large organisations these can be complex to pin down (and even at small general practice level business process will determine different information access requirements for different staff).

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

Please comment on your answer.:
2.9 This needs to be supported by a well resourced educational team to support practices. There is a risk that practices see this as another box ticking exercise without any substantial change in understanding to underpin improved data security. If CQC were to take on this role, then it would need to look at data exchange between organisations and pathways not just individual organisations.

The importance of data sharing

Proposed Consent/Opt-out Model

11 Do you have any comments or points of clarification about any of the eight elements of the model described above? If so please provide details in the space below, making it clear which of the elements you are referring to.

Which standard do you wish to comment on? - Which standard do you wish to comment on?:
4

clarification of the eight elements:
2: This needs clarification of the circumstances when it would be reasonable for a care professional to override a patient's wishes; for example, it may not be safe to make a referral if the patient wished for key information to be excluded.

4. The model does not allow for the possibility of opting out of your personal confidential information leaving the source organisation for purposes other than direct care (the old type 1 objection).
This appears to be based on the assumption that the issue with consent lies in the name, however this assumption has not been tested. From experience of discussing this with many patients who have opted out, the problem lies in a large central organisation holding the record. Patients trust their personal doctors, and their NHS, but not necessarily the NHS – a subtle but important distinction.
Renaming HSCIC NHS Digital does not, of itself, make the organisation 'trusted'. There has already been much publicity about previous inappropriate sharing of data and lack of knowledge about what data had been shared with whom and a name change may appear as an attempt for the HSCIC to distance itself its past. Also the name "NHS digital" could be confused with "http://www.digitalhealth.net/" and http://digitalhealth.london/about-us/) which are commercial ventures. A google of "NHS digital" brings up many other organisations apart from the re-branded HSCIC so the name is not distinct enough for the public to understand who or what it is.
There needs to be clarity regarding what constitutes research, what constitutes managing the NHS and what is commercial use. The reality is that these areas often overlap substantially. Will the HRA definition of research is used which only has three simple questions which would http://www.hra.nhs.uk/research-community/before-you-apply/determine-whether-your-study-is-research/ or the broader HEFCE definition of research? How would market research be considered?
The Secretary of State requested a simple system, and this is understandable, however we would do well to heed the quotation often attributed to Albert Einstein: "Everything should be made as simple as possible, but not simpler." This system risks many people opting out of sharing information on a precautionary principle because the system is simplistic in its appreciation of the types of use to which data is put.
Pseudonymisation may only be one part of the adequate de-identifying of data, but pseudonymisation at source would be preferable to pseudonymisation by NHS Digital especially since there are well established robust and proven technologies already implemented by the main GP suppliers and other organisations including the Office of National Statistics and Public Health England and the HSCIC it. Pseudonymisation-at-source (i.e. by the source system) would reduce

unnecessary flows of personal confidential data to unconnected third parties and reduce unnecessary costs

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

Please comment on your answer:

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

Organisation support:

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

patient or service user, where would you look for advice :

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?

What are your views about how the transition from the existing objection regime to the new model can be achieved?:
If the abolition of the type 1 opt out goes ahead then, the task of explaining the 180 degree change from a system of respect for autonomy and choice to a compulsory flow of inbound data to the HSCIC/NHS Digital to patients is huge (especially for those practices who had previously proactively contacted patients to offer them choices.) Since the inception of care.data the EMIS NUG chair's practice has sought explicit choice form patients registering regarding sharing of data to HSCIC: 1066 have given explicit consent, 818 have expressed explicit dissent. Will the express dissent of these patients still be respected, and if not who will be responsible for informing them and explaining why?
The loss of patient opt-outs seems to be contrary to the statement at the beginning of the report "people should be able to opt out of their personal confidential data being used for purposes beyond their direct care unless there is a mandatory legal requirement or an overriding public interest". The subtlety of the Secretary of State being able to legally demand patients' data may be lost on the average patient. There is also a risk to public trust is promises made two years ago are then easily cancelled shortly afterwards for no compelling reason. How can patients are reassured that the choices which are being offered now will not be superseded by a new health secretary or government.
If the information is to be passed without right of opt-out to HSCIC/NHS Digital then this body will need to have very transparently independent governance. The current "Independent Information Governance Oversight Panel" has nearly half of its membership on the payroll of either HSCIC/NHS digital or HRA. Whilst these people are no doubt motivated to act with integrity this does not give an obvious and transparent independence.
For GP data controllers they will need to be clear about the responsibilities that they bear. Once the data passes to HSCIC/NHS Digital, using the provisions of the Health & Social Care Act, NHS England will become the data controller with all the relevant responsibilities regarding fair processing information to patients It needs to be made clear that, in the event of a data breach either by HSCIC/NHS Digital or someone to whom they have supplied the information, the liability will lie with NHS Digital/NHSE.
Any subject access requests regarding these data must be handled by NHS Digital/NHSE, rather than the patient's GP.
The opt-outs presented as an information profile appear clearer than the tick-box format.
It is unclear if this document is suggesting that HSCIC will be the only means of pseudonymising data and obtaining pseudonymised data. This would have implications for other organisations who currently obtain pseudonymised data directly from the data controller for research or audit which is de-identified according to the ICO code of anonymisation (2012).

Equality Issues

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?

Please comment on your answer:
Yes. Vulnerable people are often most concerned regarding their data, but also most in need of good sharing of information for the purposes of direct patient care. If the proposed changes to the opt-out model go forward where a patient cannot dissent from information being uploaded to HSCIC/NHS Digital then the only way to prevent this information going will be not to enter it in the record. This will mean that it is not available to other clinicians, whether in another or the same organisation, putting vulnerable people at risk.
Explaining the new model and the changes from the previous model will pose a significant challenge for patients whose first language is not English, for children, for those with dementia and disabilities, for those who are living abroad, for students and for those with mental health illnesses who may be in hospital. It is unclear who will have the task of communicating the changes to patients and how this will be resourced. It will be difficult for GPs to explain the purposes for which the data may be used (which are not clearly articulated) alongside the purposes for which it may not be used if the patient opts out (which appear to be limited to two ill-defined purposes). This is especially difficult when it appears that the opt outs can be overridden by a direction from NHS England to the HSCIC (such as the one issued for care data.

Replacing two clear opt outs (type 1 and type2) with two opt outs based on ill-defined purposes is a fundamentally flawed approach because of the lack of definition of the purposes and hence it should be reconsidered. The government needs to be much clearer about what it plans to do with personal confidential data and any limitations there will be. For example, will the data be shared for purposes which the public may be uncomfortable with for example with the DWP to investigate benefit fraud; will it be shared with the tax office or with the police and used for counter-terrorism. If so, then patients must be informed. This may well then affect patients with protected characteristics who may be too afraid to seek medical help. Some patients with learning difficulties or children may find it very difficult to understand that the hitherto confidential nature of the relationship with their doctor will be replace by a system that may copy all their medical information in identifiable format to an organisation (NHS Digital) they are unlikely to have ever heard of.

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.

Please comment on your answer: