Response ID ANON-2BBS-3U12-M

Submitted to **New data security standards and opt-out models for health and social care**
Submitted on **2016-09-06 15:28:14**

Foreword

Introduction

1 Please tell us which group you belong to.

Group title:
Special Interest Group

Other - Please specify:
BCS Primary Health Care Specialist Group (PHCSG)

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:
The Primary Health Care Specialist Group (PHCSG) is very interested in participating in further discussions and in attending meetings.

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?:

Comments:
Applicable to all the proposed standards.
The Review itself discusses Leadership People Processes and Technology as a necessary means of establishing confidence in the ability and willingness of the NHS to manage patient data securely and maintain confidentiality
Neither establishing trust nor the four areas above are mentioned in the Consultation, but we would suggest will need to be addressed in the final DH response to the Review along with some suggestions on achieving the desired end effects.

On the 10 Standards.
PHCSG welcomes the application of standards across the NHS and social care including private providers, but has some concerns as to how these can be implemented and monitored: we would welcome further clarification on the time scales envisaged, and the relationship of the introduction of the standards to the establishment of Public Trust and how the Department and NHS England plan to convey this to the Public.
Standards 1-4
Some of the definitions are unclear and clarification would be helpful e.g references to “staff” and in Standard 3 data security training and annual mandatory testing: it is unclear as to the definition of “staff” – is this clinical/front-line staff or does it include IT and support staff with potential access to patient data in the course of their non-clinical duties?
Is the mandatory annual testing intended to be role-specific or so general that it will risk being seen as a tick box exercise?
Standard 4
Although this is desirable, there may be problems in implementation and guidance will need to be given in the DH’s final plans.
a. Access for staff needing it and removal of access when no longer a need. There is a problem with sessional and temporary workers and supernumeraries who do not fit the procedures for RBAC (Role Based Access Control) smartcards e.g. locums and agency workers: IT contractors: medical students. This leads to undesirable work-arounds and lack of clarity in the audit trail as to who accessed or altered the clinical record.
b. It is not clear whether existing record systems show access to a record and if so whether the nature of that access is recorded e.g. if results are filed into a record, this could be recorded as access (record has been updated)
c. If existing digital record systems do not record all access – as opposed to all updates/changes – will this Standard prevent the use of such systems?
d. If this Standard applies to all patient records, how would DH recommend it should be applied to non-digital records?
Providing an audit trail of everyone who has accessed a record might need the software to be extensively modified and needs a mechanism for recording the role of the individual accessing the record (which means the software has to be able to identify them and record viewing as well as making changes) and a means of informing the data subject.

Standard 8
While the use of “unsupported operating systems, software or internet browsers” is undesirable, clarity in the definitions and implications would be welcome. Does this include, for example, Open Source software and OS (Linux) and Apps?

Technology and use of technology are changing rapidly, and the PHCSG feels that it would be unfortunate if this Standard had the effect of inhibiting innovation in the NHS.

As defined at present, Standard 8 would appear to demand major software and hardware upgrades whenever a supplier – such as Microsoft – issued a new OS or software version or withdrew support from a previous version. Although resources were not a part of the Review, this is an issue which will need to be addressed by the DH and NHS England when Standards are implemented.

Many organisations – including general practice – use software for business and other purposes which is not part of their EHR systems e.g. accounts packages, bibliography, revalidation software. Would such software be included in Standard 8?

Consideration needs to be given to how risks can be mitigated (e.g. by isolating the systems being used) in the process of updating or replacing such unsupported systes in the immediate, medium and – where replacement is impossible – long term, and at a strategic level how the existence of these systems will impact both on the capability of the NHS to protect patients and the public perception.

In general, it is not clear that the full implications of the recommendations have been fully considered in the Consultation – and the important question of lack of Trust has not been addressed, but will need to be in the final DH response to the Review.
In particular, the storage of data and the terms on which it could be accessed or distributed for managing the NHS and Research and health improvement.
See comments Q6

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.:
see also response to Q4
3. “All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit “
This is a very heavy increased demand on small organisations such as general practice.
Who is included in “all staff”, and would the mandatory training be different for different degrees of access? In general practice, staff have many different roles - & they change!
The resource cost of applying this Standard, including time commitments, might be excessive for many organisations.
The IG Toolkit – if it is to be the source of training – would require very extensive revision and repurposing: would it not be better to increase resources in the current training site – which would also be able to be more agile in updating and expanding training materials?

4. “Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals “
There are problems with authorising and recording access for and by temporary staff and supernumaries such as medical students which need to be addressed both in organisational and IT system terms .
There may be problems with existing systems and with specifications for new systems.
8.” No unsupported operating systems, software or internet browsers are used within the IT estate “
• This might cause major problems in general practice (extensive use of calculators and need for non-clinical software such as banking and accounts).
• Does this imply that NHS systems demanding the use of unsupported software/OS (such as IE6/7 and XP) would need to be changed immediately? If so, how will change be resourced? (software, hardware, suppliers, contract changes, training?)
• Strict application may inhibit innovation and the use of new technology as yet unknown
• Without clarification of “support” it is not clear whether this Standard would prevent the use of Open Source software
• Is it known how many systems depend on “unsupported software” – and what is meant by supported or unsupported? NHS? Commercial companies? Licenses? CSUs?
• Would this affect the Integrated Care Records needed by new ways of working?
10.” Suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian’s Data Security Standard “
• How would this apply to existing contracts, and how could a data-processor (the supplier) be held accountable for data breaches rather than the Data Controller?
• GPs are Data Controllers but have no contractual connection with the GP system suppliers who are the data processors: how will the contractors – whoever they may be – be made accountable for setting the contracts?

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

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.:
Some of the recording standards might be hard to implement on paper-based records e.g. who has accessed the record.
Social care depends on large numbers of care workers having direct access to a small number of patients/clients and their personal care records: clarification would be welcome on how it is envisaged some of the standards – and sharing – would be managed in a non-digital sector which is already underfunded and under stress and what support would be provided to this sector.

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.:
2.9 “The review also heard from the primary care community in particular that they would value support to meet the standards provided by a refreshed IG toolkit and HSCIC. HSCIC could, for example, use the new toolkit to identify organisations that would benefit from additional support, and also to put organisations in touch with each other for peer support. HSCIC should work with other regulators to ensure that there is coherent oversight of data security across the health and social care system “

‘The primary care community’ includes both general practice (highly computerised and used to data security & confidentiality issues) and other organisations such as community care & social services (less familiar with computerisation and the data
security & confidentiality issues arising from the change from paper to digital).
Advice and support need to be tailored to different groups of recipients to prevent compliance becoming a tick-box exercise
Clear advice on the implementation of the standards and supported educational/testing materials would be welcome.

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

No

Please comment on your answer.:
2.8
• The role of CQC in including the standards in their inspection regime would seem logical: once this is included, it would be helpful if the organisations being inspected had clear information on what was required and CQC inspectors were fully educated in security and the application of the standards (it has been known for GP practice inspection teams to lack any members with specialist knowledge of general practice).
• Using the outcomes of submissions to HSCIC for approval of status using the new IG Toolkit to identify organisations needing an early CQC inspection suggests that the new IG Toolkit will be designed to produce this information. Elsewhere it is suggested that the re-designed IG Toolkit will be designed to provide guidance, training material and support for mandatory staff tests. Consideration needs to be given to the purpose of the IG Toolkit which will affect its design, content and uses for central and regulatory purposes.
• Training material is currently provided on a separate website which is user-friendly and much appreciated: rather than incorporating material into the IG Toolkit, consideration should be given to developing the existing training material and pointing to it from the toolkit: this would have the additional advantage of being able to be more rapidly developed or changed with changing training requirements.
2.9
“...HSCIC should work with other regulators to ensure that there is coherent oversight of data security across the health and social care system “
• If HSCIC/NHS Digital is to become a regulator in addition to CQC, the relationships between the various regulators and their fields of responsibility need to be agreed and defined in order
• to prevent costly duplication of effort with a possibility of inconsistent outcomes from different regulators and
• to decrease the regulatory overload on service providers

Clarification of the apparent intent for HSCIC to act as a regulator would be welcome

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?:

clarification of the eight elements:
General .
Definition of “Personal Confidential Data”
Continual introduction of new terms into reviews and consultations without immediately available definitions or rationale is confusing to the public and should be

avoided whenever possible.
If such new terms are needed, clarification needs to be provided in the Review of Consultation.
1. “You are protected by the law
• It would be useful to have a reference or list of what this protection is
2. “Information is essential for high quality care.
Doctors, nurses and others providing your care need to have some information about you to ensure that your care is safe and effective.”
• Is the need for information for high quality care limited – as implied – to the need for direct care providers to have ‘some information about you’?
• This appears to be combining direct care of the individual patient and secondary uses of identifiable data. The two are different and need to be considered separately
“However, you can ask your health care professional not to pass on particular information to others involved in providing your care.”
In a point to point referral e.g. referral for a gynaecological problem to a
• gynaecologist, omiting irrelevant clinical information is not a problem. It could, however, be a Clinical Safety Issue in some circumstances – both for patient and for care providers e.g. severe mental health problems not under control, HIV status/medication, adverse reactions to medication prescribed for a withheld diagnosis.
• Technically, is it possible to label parts of the individual patient record as not to be shared with other healthcare providers? Is this a commitment to introduction of the sealed envelop?
• In a digital age with integrated care It is not known what the episode requiring care will be in advance, so it is equally impossible for either patient of doctor to be sure that the information not being shared will not be highly relevant to the safe care of the individual patient
• We would suggest that the medical, legal and ethical implications of incomplete records when there is a justifiable assumption that the record is complete should be further examined and made clear before this plan is adopted. Both The public and the clinicians providing the health or social care need to be clearly informed of the risks and implications.
4. “You have the right to opt-out of your personal confidential information being used for these other purposes beyond your direct care.
This opt-out covers:
d) Personal confidential information being used to provide local services and run the NHS and social care system.

For example:
• NHS England surveys, for example to find out patients’ experiences of care and treatment for cancer
• regulators and those providing care checking its quality
• NHS Improvement auditing the quality of hospital data.
e) Personal confidential information being used to support research and improve treatment and care.

For example:
• a university researching the effectiveness of the NHS Bowel Cancer Screening Programme
• a researcher writing to an individual to invite them to participate in a specific approved research project

• This choice could be presented as two separate opt-outs. Or there could be a single opt-out covering personal confidential information being used both in running the health and social care system and to support research and improve treatment and care.”
The choice of examples is peculiar and incomplete and unlikely to be helpful in commenting on this consultation.
The language would make it difficult to opt out of ‘Personal confidential information being used to provide local services and run the NHS and social care system.’ or
‘support research & improve treatment & care’ (which are not the same thing)
The PHCSG consider that the choice of wording for the proposed dissent to the use of identifiable personal confidential information is confusing and appears to be limited to situations to which patients are unlikely to refuse consent while not including other uses – including commercial uses and combination with other data held by government departments and due to be shared between them.
The explanation of the implications needs to be further considered and there needs to be a clearer description of and commitment to methods of handling data not covered by the two consent/dissent uses in the new consent model e.g. whether data will normally be distributed to suitable applicants as an entire database, or as a statistical sample, or only accessed in a secure environment
7. “The opt-out will not apply to anonymised information.
The Information Commissioner’s Office has a Code of Practice that establishes how data may be sufficiently anonymised that it may be used in controlled circumstances without breaching anyone’s privacy. The ICO independently monitors the Code.
The Health and Social Care Information Centre, as the statutory safe haven for the health and social care system, will anonymise personal confidential information it holds and share it with those that are authorised to use it. (my bold)
By using anonymised data, NHS managers and researchers will have less need to use people’s personal confidential information and less justification for doing so.”

The information that the identifiable personal data will be acquired by the HSCIC without any option to prevent this happening is reinforced by 8 – the long list of circumstances where an opt-out will not apply (bullet 2): there is no indication in this that this is a total change from the current system (preventing personal identifiable information in GP records being uploaded to the HSCIC (Type 1 objection) and/or being distributed by the HSCIC (Type 2 objection)
Nor is there any suggestion that this significant change is open to Consultation – only the wording of the proposed new opt-outs from two specific, very ill-defined end uses.

8.“The opt-out will not apply where there is a mandatory legal requirement. This includes:
• the Care Quality Commission, which has powers of inspection and entry to require documents, information and records;
• the HSCIC, the statutory safe haven, which has powers to collect information when directed by the Secretary of State or NHS England;
• the NHS Counter Fraud Service, which has powers to prevent, detect and prosecute fraud in the NHS;
• investigations by regulators of professionals;
• coroners’ investigations into the circumstances of a death, i.e. if the death occurred in a violent manner or in custody;
• health professionals must report notifiable diseases, including food poisoning;
• the Chief Medical Officer must be notified of termination of pregnancy;

• employers must report deaths, major injuries and accidents to the Health and Safety Executive;
• information must be provided to the police when requested to help identify a driver alleged to have committed a traffic offence; or to help prevent an act of terrorism or prosecuting a terrorist;
• information must be shared for child or vulnerable adult safeguarding purposes; and
• health professionals must report known cases of female genital mutilation to police.
In addition the Review also sets out that the following should not be part of the opt-out:
some forms of invoice validation where there is no alternative solution, such as the use of anonymised data;
• demographic information flows (e.g. NHS number, address) into the Office of National Statistics (ONS) for the production of official statistics e.g. to look at internal migration;
• national registers of disease including cancer where there will be a new approach to informing patients about registration "

Bullet 2 – "the HSCIC, the statutory safe haven, which has powers to collect information when directed by the Secretary of State or NHS England" only applies when a Direction has been issued.
We are aware that the Care Data Program Board was planning to consult on a Single National GP Dataset after the Review was published: it is not clear whether this public consultation will now be held, and/or when or whether a Direction to HSCIC to upload all the records held in GP systems is now contemplated instead.
It is also not clear whether this would include free text, and whether such a Direction (or future plans) would include uploading all medical and social care records held electronically regardless of the organisation in which they were generated.
This appears to remove all protection against identifiable personal information being passed to the HSCIC, and the use of such data by the HSCIC – which has to follow directions issued by the Secretary of State (presumably for Health?) and NHS England.

It seems that the opt-out would only apply to very broad but undefined uses of identifiable data – not to the collection of it.
One of the themes in the Review is the lack of public trust in the ability of the NHS to manage and protect personal identifiable information: it is not clear how a mandated upload of all medical records (or only GP records?) would increase public trust.

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?

No

Please comment on your answer:
It is not clear from the Review whether the introduction of stronger penalties would apply only to data acquired from the NHS and/or social care (Review does not cover social care) or is a recommendation for penalties for "deliberate re-identification" of personal data.
Clarification and some indication of the scope of the proposed legislation would be welcome.
Would the penalties be applied to individuals or to organisations, and, as any such deliberate re-identification might be conducted outside the UK (or possibly just England) where would the legislation stand if extradition was applied for?

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 :

As a patient I would feel that my options have already been removed.
People who registered a Type 1 objection (number unknown – although the collection of numbers from each practice was authorised by the GPES IAG) did so because of lack of trust in the HSCIC and what it might do with the patient identifiable data it collected.
This review, while talking of "trust" by the public does nothing to increase it by removing the option of not allowing the entire medical record (not even just the limited data-set allowed to care.data) is not likely to increase public trust in the NHS's data handling.
It also negates a specific assurance given by the Secretary of State for Health to the public that their data would not leave their GP surgery if they objected: the Review says that this assurance will have to be abolished- but is not clear how, or on whose responsibility.
Again, clarification would be useful.

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?:
Before any change is made in the consent/opt-out model, the platform for recording and applying the new model will need to be developed following decisions on how and where it would be implemented and new arrangements made to involve and inform the public in the new model.
This would probably need to be via a variety of mechanisms and entry points (conforming to the NHS Accessibility Standards): it seems unlikely that the current registration of Type 1 and Type 2 Objections with the registered GP would be sufficient – and until the transfer of GP records by GP2GP is universal, there is a risk that, on changing practices, the consent preferences might be missed in summarising the record.

This question assumes that the Public Consultation will endorse a move from the current opt-out system (Type 1 & Type 2 objections as promised by the Secretary of State for Health) to accepting a full upload of certainly GP patient records – and possibly all medical records held electronically – to HSCIC with no possibility of the individual being able to withhold consent.

This is a drastic change, and it is hard to see a way of achieving it without first identifying the individuals who have registered Type 1 objections (not approved by the GPES IAG) and contacting them individually: HSCIC already has a list of people who have registered a Type 2 objection, and they would also need to be contacted and have the situation explained.
The legal status of the opt-outs – and the removal of the previous opt-outs – might need to be established before any action was taken.
If Trust is to be established in the management of patient confidential information, it might be politically expedient to consult specifically on this.

We can see no way of moving from the straightforward Type 1 & Type 2 opt-outs to the proposed model without :-
1. full disclosure to the public of the proposed removal of their current right to prevent their GP records being uploaded to HSCIC without their – or their GPs' - consent, even when they have expressly refused it
2. this may require a statement from the Secretary of State for Health that his assurance on Type 1 & 2 optouts has been rescinded.
3. clarification on what is intended would be useful e.g. is the intention to upload the entire patient record, including free-text (almost impossible to de-identify) or restrict the upload to Coded data?
4. Consideration needs to be given to the extent to which patients will be careful about what they say to their GPs – and GPs may be unwilling to enter information into the patients' records. Quality of both care and record might be affected and this needs to be taken into consideration.
5. In the introduction to this Consultation, George Freeman said that this was the public consultation called for in the review. If that is the case, and this is the only consultation contemplated, the remarkably poor publicicity might provoke adverse comment when and if changes are introduced and the outcomes cannot be considered to fully reflect concerns, especially from the public. With respect, is this the way to re-establish public trust?
6. What is intended for the patients who have already registered Type 1 (number unknown – but probably equal to or greater than Type 2) and Type 2 (1.2m) objections and how will it be implemented? (not sure of the legal position here)

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:
Do the proposals – especially uploading medical records to the HSCIC for linkage and de-identification – include armed services personnel and prisoners?
Prisoners in particular have greater health needs during and after internment (and probably before) but their medical records cannot be passed to the NHS after release (Rehabilitation of Offenders Act). This is important for rehabilitation – but may skew the data available for managing the NHS and research.
The PHCSG is not recommending the upload of prisoners' data to HSCIC or legislation to allow this.
Ex-service personnel may have their records passed to the NHS with their consent – but I do not know how often this happens, nor whether such records include any details of their experiences, postings , injuries and preventative measures (immunisations and prophylactics as in the Gulf War).

There is a high burden of mental and physical health issues in both groups which are not shared by the general population.
How will these be addressed without breaching confidentiality?

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: