Update on the National Data Guardian's Review and consultation, including the views of patient advocates / questions and answers

Short Update (5)

General Discussion (15)

Summary (5)

A short overview of the review, what was asked, how we responded, and what happens next

- "…to strengthen security of health and care information and ensure people can make informed choices about how their data is used."
- CQC – data security in the NHS
- Dame Fiona Caldicott – data security standards

What was asked, how we responded, and what happens next

- Most of the points were self evident
- We agreed that there needed to be further opportunities to engage on data security consent/opt-out models, and that this should include regional meetings, noting that Leeds, London and Manchester were good hubs

- Our response details:
  - Response ID ANON-2BBS-3U1U-Q
  - Submitted on 2016-09-06 11:03:38

Our actual response document

Recommendations

- Recommendation 1: The leadership of every organisation should demonstrate clear ownership and responsibility for data security, just as it does for clinical and financial management and accountability.
- Recommendation 2: A redesigned IG Toolkit should embed the new standards, identify exemplar organisations to enable peer support and cascade lessons learned. Leaders should use the IG Toolkit to engage staff and build professional capability, with support from national workforce organisations and professional bodies.
- Recommendation 3: Trusts and CCGs should use an appropriate tool to identify vulnerabilities such as dormant accounts, default passwords and multiple logins from the same account. These tools could also be also used by the IT companies that provide IT systems to GPs and social care providers.
- Recommendation 4: All health and social care organisations should provide evidence that they are taking action to improve cyber security, for example through the 'Cyber Essentials' scheme. The 'Cyber Essentials' scheme should be tested in a wider number of GP practices, Trusts and social care settings.
- Recommendation 5: NHS England should change its standard financial contracts to require organisations to take account of the data security standards. Local government should also include this requirement in contracts with the independent and voluntary sectors. Where a provider does not meet the standards over a reasonable period of time, a contract should not be extended.

Recommendations

- Recommendation 6: Arrangements for internal data security audit and external validation should be reviewed and strengthened to a level similar to those assuring financial integrity and accountability.
- Recommendation 7: CQC should amend its inspection framework and inspection approach for providers of registered health and care services to include assurance that appropriate internal and external validation against the new data security standards have been carried out, and make sure that inspectors involved are appropriately trained. HSCIC should use the redesigned IG Toolkit to inform CQC of 'at risk' organisations, and CQC should use this information to prioritise action.
- Recommendation 8: HSCIC should work with the primary care community to ensure that the redesigned IG Toolkit provides sufficient support to help them to work towards the standards. HSCIC should use the new toolkit to identify organisations for additional support, and to enable peer support. HSCIC should work with regulators to ensure that there is coherent oversight of data security across the health and care system.
- Recommendation 9: Where malicious or intentional data security breaches occur, the Department of Health should put harsher sanctions in place and ensure the actions to redress breaches proposed in the 2013 Review are implemented effectively

Recommendations

- Recommendation 10: The case for data sharing still needs to be made to the public, and all health, social care, research and public organisations should share responsibility for making that case.
- Recommendation 11: There should be a new consent/ opt-out model to allow people to opt out of their personal confidential data being used for purposes beyond their direct care. This would apply unless there is a mandatory legal requirement or an overriding public interest.
- Recommendation 12: HSCIC should take advantage of changing its name to NHS Digital to emphasise to the public that it is part of the NHS 'family', while continuing to serve the social care and health system as a whole.
- Recommendation 13: The Government should consider introducing stronger sanctions to protect anonymised data. This should include criminal penalties for deliberate and negligent re-identification of individuals.
- Recommendation 14: The forthcoming Information Governance Alliance's guidance on disseminating health and social care data should explicitly refer to the potential legal, financial, and reputational consequences of organisations failing to have regard to the ICO's Anonymisation Code of Practice by re-identifying individuals.

Recommendations

- Recommendation 15: People should continue to be able to give their explicit consent, for example to be involved in research.
- Recommendation 16: The Department of Health should look at clarifying the legal framework so that health and social care organisations can access the information they need to validate invoices, only using personal confidential data when that is essential.
- Recommendation 17: The Health Research Authority should provide the public with an easily digestible explanation of the projects that use personal confidential data and have been approved following advice from the Confidentiality Advisory Group.
- Recommendation 18: The Health and Social Care Information Centre (HSCIC) should develop a tool to help people understand how sharing their data has benefited other people. This tool should show when personal confidential data collected by HSCIC has been used and for what purposes

Open Workshops (DH/NHSE)

- Monday, 26 September, London
- Monday, 03 October, Southampton
- Monday, 10 October, Leeds

We only found out about these last night….!

For reference….

- Our response details:
  - Response ID ANON-2BBS-3U1U-Q
  - Submitted on 2016-09-06 11:03:38