An update from the Care Quality Commission and National Data Guardian
1 May 2016
Ref no: EC305

Data security reviews

Dear colleague,

In September 2015 the Secretary of State for Health commissioned us to undertake specific work in the important area of data security.

The Care Quality Commission (CQC) was asked to undertake a review of data security in the NHS. The National Data Guardian (NDG) for Health and Care was asked to develop new data security standards for the NHS and social care as well as a method for testing compliance against these.

We have completed our work and provided our reviews to the Government for consideration. We are grateful to all those who have contributed to them. We are writing to you ahead of their publication to highlight some of the key principles and actions that can be taken now in order to continue the important work of securing data.

People, processes and technology

In both of our reviews we found that across the system there is widespread

commitment to keeping data secure. Importantly, we also heard that processes work best when they are designed to support staff in delivering excellent care, rather than as an impediment to their work.

However, our reviews also identified areas where more could be done to protect against risks. These are based around three key themes that are fundamental to the secure handling of data: people, processes and technology.
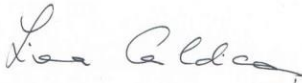
- **People**: identifying the appropriate leaders in your organisation with responsibility and accountability for data security is vital, just as it is for clinical and financial management and accountability. We would encourage you to ensure you have individuals in the roles of the Senior Information Risk Owner (SIRO) and the Caldicott Guardian at board or equivalent level, and that they are registered with the Health and Social Care Information Centre (HSCIC): http://systems.hscic.gov.uk/data/ods/searchtools/caldicott.
  Improving data security capability also depends on staff at all levels having access to training which meets a national standard. We believe that this is particularly important for board-level leaders, SIROs, Caldicott Guardians and staff with responsibility for handling data. Working with the recommendations in our reports, the HSCIC will examine how this requirement can be met from suitably qualified suppliers, helping to ensure consistency and a focus on the specific challenges faced by health and care organisations.

- **Processes**: organisations should have processes in place to prevent data security breaches and ensure that incidents or near misses are dealt with appropriately. The HSCIC's CareCERT service is able to provide the latest advice and guidance in this area.

- **Technology**: we know that technology plays an increasingly important role in many of your organisations, especially in the provision of high quality care. The reviews heard that the use of up-to-date technology with the latest protection in place is vitally important to mitigate the evolving cyber security threat. We would encourage you to ensure that your organisation's IT estate is supported in this way.

The NDG's new data security standards have been designed around these themes so that they are clear and can be implemented by organisations across the system. The standards are designed to be as relevant to GPs and smaller care providers as they are to large NHS trusts.

Alongside these, the NDG report will also recommend a new opt-out model to apply across the health and care system where data is shared for purposes beyond direct care. In the meantime, we would encourage organisations to ensure there is a clear view of all data flows and the purposes and legal bases for these.
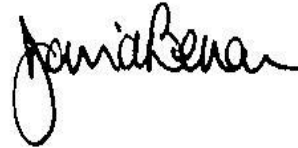
We look forward to sharing our full findings and recommendations with you and to continuing to work with you to ensure that patients and service users can trust that their health and care data is kept safe and secure.

Yours sincerely,

Dame Fiona Caldicott, MA FRCP FRCPsych
National Data Guardian

David Behan
Chief Executive
Care Quality Commission