Published on *The National Law Review* https://natlawreview.com

UK Government Considering New Patient Data Security and Research Consent Standards, Sanctions

Article By:

Philippe Bradley-Schmieg

The ***UK Government*** has opened a consultation, running until September 7, 2016, regarding how UK ***National Health Service (NHS)*** patient data should be safeguarded, and how it could be used for purposes other than direct care (*e.g.* scientific research).

The consultation comes after two parallel-track reviews of information governance and data security arrangements in the NHS found a number of shortcomings, described below. The Care Quality Commission (CQC) and the National Data Guardian (NDG, led by Dame Fiona Caldicott) made a range of recommendations, including new security standards, stronger inspection and enforcement around security lapses and re-identification of anonymized patient data, and an eight-point process around assuming and respecting patient consent decisions.

Following the public consultation, the new security standards could eventually be required and audited by government inspectors from the CQC, and imposed under revised standard NHS England contract terms. CQC inspectors could potentially act on tip-offs from NHS Digital (formerly known as the NHS Health and Social Care Information Centre, 'HSCIC'). Those tip-offs could be based on low scores obtained by organizations in their annual NHS Information Governance Toolkit (IGT) self-assessments. The IGT, which the reviewers said should be redesigned, applies both to NHS bodies and their commercial vendors.

The new consent model, meanwhile, could provide more streamlined, system-wide consents for use of patient data for purposes including quality assurance and research.

The CQC and the NDG's findings and twenty-four recommendations were jointly presented in a covering letter to the UK government, available here, and fuller reports, available here and here (CQC and NDG, respectively). This post provides a brief summary of their main findings and recommendations. For the consultation questions themselves, see here.

The CQC, which regulates the provision of healthcare in the UK, examined data security practices of 60 UK hospitals, general practice ("GP") clinics, and dental practices. It found that:

- Whilst there was "widespread commitment" to data security, training quality was variable, and policies were not always reliably put into practice;

- Data security systems and protocols were not always user-friendly, leading to insecure workarounds being used to ensure timely patient care, particularly in emergency settings. Meanwhile, computer hardware and software that can no longer be supported should be replaced as a matter of urgency;

- Lapses in patient data security were taken seriously, but lessons were not always learned or widely shared;

- Benchmarking against peer organizations, and sharing of best practice, was inadequate, and data security audit practices should be improved to match the level of rigour undertaken by financial audits;

- The move to a paperless NHS (using electronic medical records) is solving many data security issues, but care is needed to avoid large-scale electronic data losses; and

- As care becomes more integrated between different organizations and arms of the care system, improvements must be made to the ease and safety of sharing data between services.

Adding to the CQC's findings, the NDG reported that:

- While there is still limited public knowledge about how data is used in health and social care, people have a high degree of trust that the NHS will safeguard their data. However, they want reassurance about security when their data is moved outside the NHS. Some want harsher sanctions for intentional or malicious breaches;

- GPs want a simpler explanation of what they can and cannot be doing, and assurances about the practices of organizations with which they share data;

- Strong organizational leadership, in particular from local Senior Information Risk Owners (SIRO) and other information governance leads (dubbed "Caldicott Guardians"), is valuable;

- A lack of understanding of security issues is causing people to be overly conservative, and therefore unwilling to engage in the data sharing needed to ensure integrated care; and

- Data breaches can result when people whose primary motivation is to get the job done, have to work with ineffective processes and technology.

The NDG proposed ten new high-level "data security standards" and a new consent/opt-out model for consultation. It also endorsed broader use of "proven cyber security frameworks" within the NHS and by its suppliers, calling out the UK Government's "Cyber Essentials" scheme.

Under the proposed consent model, patients could opt out of their personal data being used for purposes beyond their direct care (*e.g.* to run and improve the NHS, and support research to improve treatment and care). Preferences could be recorded once (online or in person) and respected by the many different legal entities that make up the system. Moreover, even if patients opt-out generally, they could explicitly opt in to individual projects.

The NDG argued that the consent model should however not be rolled out until after much more extensive discussion with the public about the use and safeguarding of their data.

It added that there should also be a consultation around its ten new data security standards, which could form the basis of a redesign of the IGT assurance tool. When an IGT assessment flagged that an organization (whether an NHS body or one of its vendors in the private sector) needs improvement, or is “at risk”, NHS Digital could tip off the CQC for follow-up.

Finally, the NDG also recommended tougher sanctions for intentional or malicious breaches of data security, and that thought be given as to whether there should also be stronger sanctions to protect anonymized data, including criminal penalties for deliberate and negligent re-identification of individuals.

As noted above, the recommendations and related aspects of the reports (particularly the NDG report) are being consulted on until September 7; for more details, see here.

National Law Review, Volume VI, Number 224