DAC beachcroft

DATA PROTECTION

STRATEGIC / OPERATIONAL / REGULATORY / RISK

DAC Beachcroft Associate Eleanor Tunnicliffe considers the information governance issues when implementing integrated healthcare models.

Why this area is important

To provide integrated care clinicians need access to all relevant patient data. Typically, that data is held in silos. Some Vanguards are tackling this problem by creating shared care records for health and social care professionals that include information from a patient's GP records, the latest information on hospital visits and diagnostic results.

Key issues

Many patients already assume that GPs can access their hospital records electronically and are comfortable with this. More controversial is the sharing of data across the health/social care divide; GPs report patient concerns that records may be used to inform decisions around child custody or state benefits. Some projects allow patients to choose whether such sharing happens, with other projects making more limited data available.

There is a need to gain patient buy-in and ensure they have the option to access their care record online. Concerns around data security breaches are fuelled by doubt both outside the NHS (patients and GP practices) and from within. However, as human error is the most common cause of a security breach rather than the more commonly perceived risk from data hackers, a shared record held electronically in one place, and accessible by authorised individuals, is more secure than sharing via email or paper records.

GP support is critical, with substantial amounts of data held on GP systems. Unlike providers of secondary care, GPs won't typically employ IT and information law experts to support the process of introducing a shared care record system, making communication with GPs particularly important throughout the process.

In spite of Brexit, it is likely that the requirement of the EU General Data Protection Regulation (GDPR) will be passed into UK law, but there is uncertainty around how the GDPR will be implemented. Should the NHS pay the costs of ensuring new systems are GDPR compliant when there is no legal requirement to do this, nor a commitment from the UK government to implement the GDPR? Equally, there is no sense in developing systems that might not be GDPR compliant.

Potential solutions

The main legal barrier to information sharing is not the Data Protection Act 1998 or the GDPR but the law of confidentiality; sharing identifiable patient information is permitted to inform patient care, but not for use by NHS commissioners to inform other operational decisions.

There are questions around whether distinctions between what is and is not allowed really reflect patient concerns. Undoubtedly, some patients will want to restrict processing of their data but it is uncertain whether this is the attitude of the majority. There may be other dividing lines - such as whether or not data is shared outside of the NHS family. Dame Fiona Caldicott published a Review of Data Security, Consent and Opt-outs in July - known as the Caldicott 3 report - that starts to engage with these issues. It is clear that education and dialogue will be key for getting projects off the ground. But as the Caldicott 3 report highlights, the benefits for patients and the local health economy are substantial.

More information

For advice on information governance issues, contact Eleanor Tunnicliffe on +44 (0)113 251 4732 or etunnicliffe@dacbeachcroft.com.

AT A GLANCE

- Vanguard sites are creating shared care records that enable data from GP practices, hospitals and social care to be accessed in one place
- Data is held in discrete silos meaning there are technical hurdles to overcome in achieving a unified care record
- Patients are concerned about health information being accessed by social workers or benefits officials, and so dialogue between patients and GPs is key