CCIO and Health CIO Networks discussion paper:

Data sharing and data protection in healthcare

June 2017

Introduction

It is the firm belief of the CIO and CCIO Networks that better sharing of information has the potential to save lives. That is not only true at a population level. It is also true when it comes to direct patient care.

Increasingly, giving the best treatment to a patient depends on the contributions of a number of health and social care professionals. These individuals will be drawn from a range of organisations, and from a broad geography. If they are to work together effectively, information must flow between them in a timely and efficient fashion.

At the same time, we must ensure patients understand how their data might be used. They need to be confident their privacy is being protected. We must do all we can to ensure their information is not misused.

This is not a new challenge for the health and care system. Yet it is one which has become infinitely more complex as we seek to work across organisational and geographic boundaries. This includes via sustainability and transformation plans (STPs), new models of care, and through shared care record setups.

Conflicting guidance

There is no shortage of guidance being given to health and social care on how to navigate these challenges. The issue is in fact an excess of often conflicting guidance. Care professionals are left having to decide whether non-compliance with outdated data protection laws is a bigger risk than compromising patient care by restricting information sharing.

It is a position the CIO and CCIO Networks believe is undesirable and untenable, and which national bodies must now urgently address.

SystmOne: a case in point

The problem has been thrown into stark relief by concerns over data sharing in TPP's SystmOne.

The software, used by nearly 3,000 GP practices in England, makes it possible to share information with other users via its enhanced data sharing model (EDSM) functionality. These other users could include individuals working at social care providers – local councils – as well as those at healthcare organisations.

At present, it is not possible for an organisation to say that, for instance, they are happy for the data they create to be shared with other SystmOne users in healthcare but not those in social care.

The Information Commissioner's Office (ICO) has announced it is investigating the EDSM functionality, with its concerns centred "on the fair and lawful processing of patient data on the system and ensuring adequate security of the patient data on the system". These are Principles 1 and 7 of the Data Protection Act.

A model not without safeguards

Mainstream media coverage could lead to a mistaken belief that, the minute one organisation enables EDSM functionality, any other SystmOne user can access the records created.

This is an oversimplification. In fact, there are several safeguards in place when one organisation (Organisation A) has enabled EDSM and when someone at another organisation (Organisation B) wants to access that record:

- **Someone at the Organisation B must register the patient there.** To do this, the individual must have a smartcard to gain access to SystmOne. He or she must also have the appropriate permissions to register a patient, and know some of the patient's demographic details.
- **The patient must have told Organisation A they are happy for their record to be shared with Organisation B (or C, or D).** If no consent has been given by the patient, Organisation B will not be able to view the record.
- **Organisation B must have said they are happy for their staff to view records from Organisation A**. If this permission has not been given, staff at Organisation B cannot view the record.

It is also important to understand that, if Organisation B does view the record, an immediate notification is sent to Organisation A. A full audit trail details who accessed which record and when.

It is true the system allows for an emergency override. If, for instance, a patient were in a life threatening situation then Organisation B could bypass the usual safeguards and access the record. But, again, a complete audit trail is automatically created by the system when this happens.

A confused picture

Many will feel this setup can support data sharing while maintaining appropriate levels of protection. But it is clear an argument can be made that it does not adhere to the letter of the Data Protection Act – as witnessed by the ICO's investigation.

The British Medical Association has issued guidance detailing its serious concerns about the EDSM functionality. It seems to err on the side of turning off sharing.

The ICO has said it is investigating, but urges all organisations leave the sharing functionality turned on for now. Some reassurance has also come from Keith McNeil, chief clinical information officer at NHS England, who said he and colleagues were "currently working with TPP and GP representatives to address concerns raised by ICO".

Healthcare professionals are left wondering which advice to heed. For GPs, the prospect of prosecution under the Data Protection Act can feel like a real concern.

In the meantime, mainstream media coverage which has not represented the full complexity of the issue may lead some patients to withdraw from data sharing schemes. We believe this is likely to cause more harm than good.

The need for national clarity

As Dame Fiona Caldicott's second review of information governance in health and social care made clear: "The duty to share information can be as important as the duty to protect patient confidentiality."

Following this principle at the same time as following the letter of the Data Protection Act is now extremely challenging. It does not help that the government response to Dame Caldicott's third review, which was issued in July 2016, has been further delayed by the purdah period arising from the June 2017 general election.

The legislative picture is also confusing. The Data Protection Act was first passed in 1998, and the sharing of information which is now possible in healthcare – and which we argue is desirable – is challenging to reconcile with its terms.

As information can be made available more broadly, it will be difficult for healthcare professionals to know every situation in which data might be accessed now as well as in the future. That in turn makes it difficult for patients to give informed consent. And parts of the NHS which need to see the patient record but never see the individual face-to-face – those managing immunisation or screening programmes, for instance – will never be able to easily gain the direct consent the act requires.

These issues will only become more pressing with the impending passage of the General Data Protection Regulation (GDPR, which will come into force in May 2018). This requires explicit, "unambiguous" consent for data sharing. It also involves much bigger sanctions for anyone found to be contravening data protection legislation.

Who is the controller and who is the processor?

Yet it can be challenging to identify precisely which organisations or individuals within the health and social care system are governed by the principles of the legislation.

The Data Protection Act applies to any person or body classified as a 'data controller'. Data controllers are those who determine the purposes for which data will be shared, and the way in which the data will be processed.

The Act also establishes the principle of a data processor. This is an individual or body carrying out any activity actually involving the data – so holding it, viewing it, sharing it, deleting it. The controller, however, retains full responsibility for any activity carried out by the processor.

Complicating matters further is that disclosing information to another organisation is not enough in itself to make that body a data controller.

In short, as health and social care bodies share patient data widely and in new ways, it becomes increasingly difficult to identify which bodies should be identified as the controller, and which as the processor.

The Data Protection Act does allow for joint data controllers, but such setups should be governed by written agreements – agreements that can quickly become immensely complicated in a health and care environment.

Conclusion

We believe data sharing for the benefit of individual patients and broader populations must not be stymied by lack of legislative clarity. National bodies and legislators must ensure regulations are fit for purpose. Laws must support the sharing of information as well as safeguards which respect privacy but don't restrict the chance of delivering optimum care.

This is not the current situation, and we call on national bodies to urgently address this.