

Towards a Patient Data Incident Protocol

In recent weeks, one of the UK's largest online pharmacies, in which a GP IT system supplier holds a significant shareholding and has a seat on the Board¹, has been caught selling patient details. From a patient perspective, their response has not inspired confidence.

As things currently stand, GPs cannot say to their patients, "If you were affected, you will be informed."

The Information Commissioner's Office is investigating whether there has been any breach of data protection law, but that is the extent of its remit. Other organisations, such as the General Pharmaceutical Council, are investigating within the boundaries of their remits.

However, from a patient perspective, there is no clarity as to whether an affected patient will be told. The ICO may ultimately require this to be the case, but there is no obligation on it to do so, and it will not make a decision for months - which does nothing to assist a GP who currently has a concerned patient.

There would appear to be value in a protocol between GPs and their suppliers (and onwards, to any other third parties) so that, when the protocol is activated, patients can know *with certainty* that they will be informed if they were affected - even if that notification may not come until after an investigation or a decision.

The medically ethical standard (i.e. threshold) for notification is likely to be more robust than the legal minimums enforced by the ICO. In healthcare, and concerning information about people in a medical context, professional medical ethics not data protection should inform the protocols that are enforced.

Patient outcome

When the Protocol is invoked, after a future 'Pharmacy2U-style' incident, every GP should be able to simply say to their patients: **"If you were affected by this incident, you will be notified when it has been determined that you were affected."**

This will not only provide reassurance to patients, but will minimise the impact of such incidents on GP time. How that patient outcome is delivered and the detail of what it is in it should be the subject of discussions and agreement amongst all relevant parties.

¹ <https://medconfidential.org/2015/marketing2u-was-your-health-information-sold-to-direct-marketers-by-pharmacy2u/>