A cautionary tale: doctor posts patient images online via personal smartphone

Helen Speed

Helen is Information Systems Manager with University Hospitals of Morecambe Bay NHS Foundation Trust (UHMB).

The issue of clinical staff using their own devices to record information or take pictures/images of patients, whether on smartphone or iPad, continues to rise in NHS organisations. Walk around our wards and you will find a number of iPads in use. Some have been purchased by UHMB specifically for use in clinical areas; these have security controls to protect the data on them. Some staff members are authorised to use their own devices for limited work purposes – bring your own device (BYOD) – generally for email and calendar. Again, these have security controls applied as a condition of their use. And finally, we have the largest group of all – personal devices which are not authorised for use at work. iPads are popular amongst student doctors in particular and have many educational benefits and advantages; however, all use must be lawful and adhere to UHMB policy. By way of illustration of how easy it is to go astray, here is a recent case that appeared in the press.

A junior doctor who captioned a snap of a patient's injured head 'the real Harry Potter' and posted it online has escaped suspension. The doctor admitted breaching the confidentiality of patients at University College London Hospitals by putting images on his Instagram page.

He took the photographs months earlier on his own mobile phone while working at the Whittington Hospital in Islington, north London, and St Bartholomew's Hospital in central London. The Medical Practitioners Tribunal Service said a General Medical Council (GMC) serious misconduct ruling – which the trainee general practitioner must declare on job applications – was enough punishment.

The doctor was before a 'fitness to practise' panel in Manchester, and he said: 'I feel terribly sorry and ashamed and I feel that any comment of this nature, under any circumstances or any means from a medical professional or anyone is inappropriate.'

The Tribunal told the doctor: 'To impose a sanction in addition to that finding, and on the same basis of that finding, would be, in the panel's view, disproportionate in your case.'

'It would be seeking to hold you to account a second time for matters which the panel considers have already been adequately addressed in its earlier findings.'

'Moreover, the panel has taken account of the fact that, as a young doctor in training, there is a greater likelihood that the finding of impairment might have the effect of being an impediment to the development of your career.'

The judgement does not prevent the patient from taking action against the doctor

This is a clear example of an individual using his own device in a clinical setting inappropriately. Within UHMB, we have had very few incidents to date, but there has been an incident of personal smartphone misuse for recording and emailing a patient image, and some inappropriate posting of information on social networking sites.

UHMB policy is very clear – you may not record personal confidential data on personal devices. All NHS staff are required contractually to abide by the Data Protection Act 1998 (DPA) and the Confidentiality: NHS Code of Practice. UHMB is required, under the DPA, to 'take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data', and we take this seriously.

There is good guidance available on protecting confidential information from the GMC in the Confidentiality Toolkit, available online. The Information Commissioners Office has issued very clear guidance on BYOD to ensure that that information held on BYOD devices is not accidentally or deliberately compromised. It's guidance for organisations, but is worth a read if you hold your own personal data on a smart device and would like to know a bit more about the potential hazards of doing so.

If you have any queries about use of personal devices, or any other Information Security or Information Governance matter, please get in touch with the Information Governance team via our email address information.governance@mbhcnhs.uk or via Informatics service desk.

FURTHER READING

General Medical Council Confidentiality Toolkit. Available at: http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_12_16_protecting_information.asp

Confidentiality: NHS Code of Practice, DoH 2003. Available at: <https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice>

Bring your own device (BYOD) Information Commissioners Office. Available at: http://ico.org.uk/for_organisations/data_protection/topic_guides/online/byod