



INFORMATION GOVERNANCE
BRIEFING
UNAUTHORISED ACCESS TO DATA

1. Maintaining the confidentiality of patient records is one of the absolute key requirements on organisations across the healthcare sector. Large sums of money and significant resources are spent to ensure the technical security of patient record systems and protect them against threats such as hackers and computer viruses.
2. However on a smaller scale it is frequently the actions of individuals with an approved level of access to systems who go on to commit breaches of confidentiality. Two of the most common are set out here, the first features an example where an individual looks up details of people that she knows. In the second several hospital staff access the record of a celebrity who is admitted to their hospital.
 - 2.1. A former Social Services Support Officer at Dorset County Council has been prosecuted for accessing Social Care records without authorisation. An internal investigation found that Ms Shipsey had inappropriately accessed the Social Care records without any business need to do so. The records related to four individuals known to Ms Shipsey. Michelle Shipsey of Verwood, Dorset, appeared before Poole Magistrates' Court and admitted one offence of unlawfully obtaining personal data, in breach of s170 of the Data Protection Act 2018. She was sentenced to a 6 month conditional discharge and ordered to pay costs of £700. <https://ico.org.uk/action-weve-taken/enforcement/>
 - 2.2. In 2018 a hospital apologised to Sir Alex Ferguson after staff were accused of spying on his medical records while he was having treatment for a brain haemorrhage. The former Manchester United manager had emergency surgery at Salford Royal hospital and was kept in intensive care after he collapsed at home in May. The hospital said several staff were under investigation "in relation to an information governance breach". The Sunday Times reported that two doctors, a senior consultant and at least two nurses accessed Ferguson's records despite not being responsible for his care. <https://www.thetimes.co.uk/article/doctors-spied-on-ailing-sir-alex-ferguson-in-salford-royal-hospital-rwn9gjcl>
3. In both the cases above the staff involved had approved access to a system but not the specific authorisation to access any record they wanted to. All modern electronic record systems have audit trails that allow all actions to be detected and evidence of activity can be provided to support disciplinary cases and where necessary criminal prosecutions. All staff should be clear that these audit trails are available and can and will be used, and if they are found to have accessed a record without authorisation they could face potentially serious sanctions up to and including a criminal record. Investigations can range from internal disciplinary, to those conducted by the ICO which may lead to a fine and court appearance, or by a professional regulator such as the GMC or N&MC, which can lead to professional sanctions.
4. It is also a clear example of why a user should never let anyone else access a system using their credentials.

If you have any queries about this, or any Information Governance issue, please contact the N3i service desk marking your query IG. The contact details for the service desk are:

Phone: 0300 002 0001 Email: N3i.support@nhs.net Barry Jackson Head of Information Governance