

Scenario 2: Insider Threat in a Healthcare Organization

Group member:

student id:

1) Dipkumar Patel

2535265

2) Devang Zala

2534443

3) Akash Luhariya

2535266

4) Yash Kachhadiya

2543707

Legal, Ethical and Professional Issues in a Healthcare Data Breach

1. Legal Issues

What laws protect patients?

In the UK, patient information is protected by several important laws. The main legislation is the **UK GDPR** and the **Data Protection Act 2018**, which require organisations to keep personal data secure. Health information is considered "special category data" because it is highly sensitive and needs extra protection.

Another important protection is the **Common Law Duty of Confidentiality**. This means that healthcare professionals must keep patient information private unless there is a valid legal reason to share it or the patient has given permission.

The **Computer Misuse Act 1990** may also apply if an employee gains access to information they are not authorised to view or uses computer systems inappropriately.

What legal actions can be taken?

Against the Employee

If an employee deliberately accesses and sells patient data, they could face criminal charges under the Data Protection Act 2018. Obtaining or sharing personal information without permission is a criminal offence and can lead to prosecution.

They may also be prosecuted under the Computer Misuse Act 1990 if they accessed computer systems or data without proper authorisation. Depending on the seriousness of the offence, penalties can include fines and imprisonment.

In addition, the healthcare organisation may take civil action against the employee for breach of contract, breach of confidence, or any financial losses caused by their actions.

Against the Organisation

The healthcare organisation may also face legal consequences if it failed to protect patient information adequately.

The **Information Commissioner's Office (ICO)** can investigate the breach and issue significant fines if the organisation did not have appropriate security measures in place.

Patients affected by the breach may also seek compensation if they have suffered financial loss, emotional distress, or other harm as a result of their information being exposed.

2. Ethical Issues

Ethical implications of the employee's actions

The employee's actions raise serious ethical concerns. Patients trust healthcare providers with highly personal information, expecting it to remain confidential. Selling this information is a major breach of that trust.

The actions could also cause significant harm to patients. Stolen medical information can be used for identity theft, fraud, blackmail, or targeted scams. The employee chose personal financial gain over the wellbeing and privacy of patients.

Furthermore, the employee abused their position of responsibility. They had access to sensitive information because of their role, and using that access for personal benefit is unethical and unprofessional.

Ethical considerations for the organisation

The organisation must respond honestly and responsibly after discovering the breach.

One important principle is the **Duty of Candour**, which requires healthcare organisations to be open and transparent when incidents occur that could affect patients. Patients should be informed promptly so they can take steps to protect themselves.

The organisation should also focus on reducing any harm caused by the breach. This may include offering support services, providing advice on protecting personal information, and strengthening security measures.

At the same time, the organisation should accept responsibility for any weaknesses in its systems instead of placing all the blame on one individual. A fair investigation should examine both employee misconduct and any security failures that made the breach possible.

3. Professional Issues

Professional responsibilities of employees

Healthcare workers and other staff members have a professional duty to protect confidential information.

Many professions have codes of conduct that require employees to maintain privacy and act in the best interests of patients. For example, doctors follow guidance from the General Medical Council (GMC), while nurses follow the Nursing and Midwifery Council (NMC) Code.

Employees should only access information that is necessary for their role. Accessing records out of curiosity or for personal reasons is a clear violation of professional standards.

Staff members also have a responsibility to report suspicious behaviour. If they believe a colleague is misusing patient data, they should raise concerns through the organisation's whistleblowing procedures or Freedom to Speak Up channels.

Consequences for Professional Standing

A serious data breach can have long-term consequences for an employee's career. Healthcare professionals may be referred to their professional regulator and could face disciplinary action, suspension, or removal from the professional register. In some cases, this can prevent them from working in healthcare again.

Detection and Prevention Measures

Healthcare organisations can reduce the risk of insider threats by using a combination of technical, administrative, and monitoring controls.

Area	Examples of Measures
Technical Controls	Role-Based Access Control (RBAC), NHS Smartcards, Data Loss Prevention (DLP) systems, and Security Information and Event Management (SIEM) tools to monitor unusual activity.
Administrative Controls	Staff training, regular security awareness programmes, DBS checks, reference checks, and strict procedures when employees change roles or leave the organisation.
Monitoring and Auditing	Continuous monitoring of system activity, regular audits of access logs, and compliance with NHS Digital and National Cyber Security Centre (NCSC) guidance.