

Insider Threat in a Healthcare Organization

Group : 2

Group member :

- | | |
|--------------------------|------------------|
| 1. Tushar Solanki | (2536692) |
| 2. Diya Patel | (2532979) |
| 3. Priti Bhoi | (2540464) |
| 4. Dhaval Rami | (2528086) |

Insider Threat in a Healthcare Organization

1. Legal Issues

a. What laws protect patient information?

Several laws protect patient health information and privacy:

- **Health Insurance Portability and Accountability Act (HIPAA)** (United States): Protects patients' medical records and personal health information (PHI) and requires healthcare organizations to implement safeguards.
- **General Data Protection Regulation (GDPR)** (European Union and UK GDPR): Protects personal data, including health information, and imposes strict requirements on organizations handling such data.
- **Data Protection Act 2018** (United Kingdom): Implements and supplements UK GDPR requirements.
- Other national healthcare privacy laws may also apply depending on the country.

b. What legal actions can be taken against the employee and the organization?

Against the Employee:

- Criminal prosecution for unauthorized access, theft, or sale of confidential data.
- Civil lawsuits from affected patients seeking compensation for damages.
- Employment termination and loss of professional licenses or certifications.
- Fines, imprisonment, or both, depending on applicable laws.

Against the Organization:

- Regulatory investigations and penalties for failing to protect patient data.
 - Civil lawsuits from affected patients.
 - Mandatory breach notification requirements.
 - Reputational damage and potential loss of business.
 - Corrective action plans imposed by regulatory authorities.
-

2. Ethical Issues

a. Ethical implications of the employee's actions

The employee's actions are ethically unacceptable because they:

- Violated patient privacy and confidentiality.
- Breached the trust patients place in healthcare providers.
- Used privileged access for personal gain.
- Potentially exposed patients to identity theft, discrimination, or other harms.
- Undermined the integrity and reputation of the healthcare profession.

Key ethical principles violated include:

- **Confidentiality**
- **Integrity**
- **Trustworthiness**
- **Respect for persons**
- **Professional responsibility**

b. Ethical considerations guiding the organization's response

The organization should:

- Act transparently and honestly about the breach.
- Notify affected patients promptly.
- Cooperate fully with regulators and law enforcement.
- Protect patients from further harm.
- Investigate the incident fairly and thoroughly.
- Strengthen security controls to prevent recurrence.
- Maintain accountability while respecting employee rights during the investigation.

The response should prioritize patient welfare, privacy, and public trust.

3. Professional Issues

a. Professional obligations of employees handling sensitive information

Employees have a duty to:

- Maintain confidentiality of patient information.
- Access only information necessary for their job responsibilities.
- Follow organizational security policies and procedures.
- Protect passwords and access credentials.
- Report suspected security incidents or policy violations.
- Comply with legal and ethical standards governing healthcare data.
- Complete required security and privacy training.

Healthcare professionals are entrusted with sensitive information and must handle it responsibly at all times.

b. Measures to detect and prevent insider threats

Organizations can implement the following measures:

Technical Controls

- Role-Based Access Control (RBAC) to limit access to necessary data.
- Multi-Factor Authentication (MFA).
- Data Loss Prevention (DLP) systems.
- Security Information and Event Management (SIEM) tools for monitoring suspicious activity.
- User and Entity Behavior Analytics (UEBA) to detect unusual access patterns.
- Encryption of sensitive data.

Administrative Controls

- Regular security awareness and ethics training.
- Background checks for employees.
- Clear policies regarding data access and acceptable use.
- Separation of duties to reduce opportunities for abuse.
- Periodic access reviews and audits.

Monitoring and Detection

- Audit logs of all patient record access.
- Automated alerts for unusual data downloads or access outside working hours.
- Regular compliance assessments and internal audits.
- Whistleblower and reporting mechanisms.

Incident Response

- Established insider threat response procedures.
 - Rapid investigation and containment processes.
 - Coordination with legal, HR, and cybersecurity teams.
-