PIK
LONDON

PARTNERS IN KNOWLEDGE UK LTD
Suite No. 129
295 Chiswick High Road
LONDON W4 4HH

Integrated Safety and Security Leadership in the Healthcare

PIK-0726 TRK-IST-2

WESTMINSTER
BUSINESS COUNCIL

Place	: Istanbul	**Venue**	: Levni Hotel (Hoca Pa?a, Mahallesi, Ankara Cd. No:12, 34110 Fatih/?stanbul, TURKEY) - TBC		
Start Date	: 20-07-2026	**End Date**	: 31-07-2026	**PPP**	: £4950

Integrated Safety and Security Leadership in the Healthcare
PIK-0726 TRK-IST-2

If you can't train them, you can't blame them!

Short Description:

This intensive 10-day workshop is designed to equip healthcare managers with the knowledge, tools, and leadership skills necessary to ensure a safe and secure environment for patients, staff, and visitors. Participants will explore key concepts in healthcare safety, risk management, emergency preparedness, cybersecurity, and regulatory compliance, with a focus on practical application in real-world healthcare settings. Through interactive sessions, case studies, group discussions, and scenario-based exercises, the workshop emphasizes proactive risk identification, crisis response, and building a culture of safety. By the end of the program, participants will be able to lead safety initiatives, respond effectively to incidents, and integrate security practices into daily healthcare operations.

Course Overview:

Workshop Objectives

- Develop a comprehensive understanding of healthcare safety & security principles.
- Identify and mitigate risks in clinical and operational environments.
- Strengthen emergency preparedness and incident response capabilities.
- Enhance knowledge of data protection & cybersecurity in healthcare.
- Build leadership skills to foster a culture of safety and accountability.

Target Audience

- Healthcare facility managers.
- Hospital administrators.
- Clinical department heads.
- Risk and compliance officers.
- Health & safety officers.
- Security managers in healthcare settings.
- Quality improvement and patient safety professionals.

Program Outline:

Workshop Layout

DAY-1: Introduction to Healthcare Safety & Security

- Overview of safety & security in healthcare.
- Key challenges and emerging risks.
- Roles and responsibilities of managers.
- Regulatory frameworks and standards.

- Building a safety culture.

DAY-2: Risk Management Fundamentals

- Risk identification techniques.
- Risk assessment tools.
- Hazard analysis in healthcare settings.
- Risk prioritization and mitigation strategies.
- Documentation & reporting.

Day 3: Patient Safety & Clinical Risk

- Common patient safety incidents.
- Medication safety practices.
- Infection prevention and control.
- Clinical error reporting systems.
- Root cause analysis.

Day 4: Workplace Safety

- Occupational health hazards.
- Staff safety and wellbeing.
- Handling workplace violence.
- Ergonomics and injury prevention.
- Safety audits and inspections.

Day 5: Emergency Preparedness

- Types of healthcare emergencies.
- Emergency planning frameworks.
- Disaster response coordination.
- Communication during crises.
- Simulation exercises.

Day 6: Physical Security Management

- Access control systems.
- Surveillance and monitoring.
- Protecting patients and staff.
- Managing visitors and contractors.
- Security incident response.

Day 7: Cybersecurity in Healthcare

- Common cyber threats.
- Data protection principles.
- Securing patient records.
- Incident response for cyber breaches.

- Staff awareness and training.

Day 8: Legal & Ethical Considerations

- Healthcare laws & regulations.
- Patient confidentiality and privacy.
- Ethical decision-making.
- Liability and accountability.
- Compliance strategies.

Day 9: Leadership in Safety & Security

- Leading safety initiatives.
- Communication and teamwork.
- Change management.
- Building a reporting culture.
- Performance monitoring.

Day 10: Integration & Continuous Improvement

- Safety and security integration.
- Quality improvement frameworks.
- Key performance indicators.
- Continuous monitoring and evaluation.
- Action planning and wrap-up.

Case Study: Managing a Cybersecurity Breach in a Hospital

A large urban hospital experienced a ransomware attack that compromised its electronic health record system. The attack led to system downtime, forcing staff to revert to manual documentation. Patient care was disrupted, appointments were cancelled, and emergency cases had to be diverted to nearby facilities.

The breach occurred due to a phishing email opened by an employee, which allowed attackers to access the hospital's network. The IT team detected unusual activity, but response delays worsened the situation. Communication breakdowns between departments further complicated recovery efforts.

Hospital leadership faced multiple challenges: maintaining patient safety during system outages, managing public communication, complying with legal reporting requirements, and restoring systems securely. Post-incident analysis revealed gaps in staff training, outdated security systems, and lack of a coordinated incident response plan.

In response, the hospital implemented stronger cybersecurity protocols, mandatory staff training, improved incident response procedures, and regular system audits. Leadership also emphasized building a culture of accountability and preparedness to prevent future incidents.

Group Discussion Questions:

1. **What were the key failures that led to the incident?**
2. **How could the hospital have minimized the impact of the attack?**
3. **What long-term strategies should be implemented to prevent recurrence?**