1. Chief Information Security Officer (CISO): Responsible for developing and implementing the information security management system (ISMS), ensuring compliance with relevant regulations, and managing information security risks.
2. IT Manager: Responsible for managing the day-to-day operations of the clinic's IT infrastructure, ensuring its reliability, availability, and security.
3. Data Protection Officer (DPO): Responsible for ensuring compliance with data protection regulations, such as GDPR, and overseeing data privacy and security within the organization.
4. Medical Director: Responsible for ensuring the confidentiality, integrity, and availability of medical information, and maintaining compliance with healthcare regulations.
5. Human Resources Manager: Responsible for ensuring that all employees are aware of their information security responsibilities and receive appropriate training to handle sensitive information.
6. Compliance Officer: Responsible for ensuring that the organization adheres to regulatory requirements, such as HIPAA, and takes appropriate measures to manage risks associated with non-compliance.
7. Information Security Analyst: Responsible for conducting risk assessments, identifying vulnerabilities, and implementing security controls to mitigate risks.
8. Network Administrator: Responsible for configuring and maintaining the organization's network infrastructure, including firewalls, switches, and routers, and ensuring its security.
9. Application Developer: Responsible for developing and maintaining software applications used by the organization and ensuring their security and compliance with relevant regulations.
10. Administrative Staff: Responsible for handling sensitive information in accordance with established policies and procedures, and reporting any potential security incidents to appropriate personnel.