

Healthcare M&A Security Checklist

CREATING AN INCIDENT RESPONSE PLAN

- ☐ Define roles and responsibilities for incident response
- ☐ Determine protocols for communication
- ☐ Develop containment strategies
- ☐ Test plan effectiveness through simulated incidents

ENSURING VENDOR RISK MANAGEMENT

- ☐ Verify that third party vendors have implemented security measures and adhere to industry standards
- ☐ Review vendor contracts for data protection and security requirements
- ☐ Establish a program for managing vendor risk
- ☐ Conduct regular assessments and monitoring

DEVELOPING A SECURITY AWARENESS CULTURE

- ☐ Educate and train employees from both organizations on security and data protection best practices
- ☐ Raise awareness of potential threats, social engineering attacks, and management of sensitive data
- ☐ Create a reporting mechanism for security incidents, suspicious activity, and policy violations

IMPLEMENTING AUTHENTICATION & ACCESS CONTROLS

- ☐ Require multi-factor authentication (MFA) for access to vital resources
- ☐ Employ the principle of least privilege (PoLP) to restrict access to only what is required
- ☐ Review and update user access permissions frequently

ENGAGING LEGAL & COMPLIANCE

- ☐ Involve legal and compliance experts who specialize in healthcare regulations

ESTABLISHING COMMUNICATION & COLLABORATION CHANNELS

- ☐ Establish explicit communication channels between key stakeholders
- ☐ Promote collaboration and information sharing to rapidly identify security hazards
- ☐ Communicate security updates, policy changes, and progress on a regular basis to all employees

MAINTAINING CONTINUOUS MONITORING & AUDITING

- ☐ Create mechanisms to detect anomalies, unauthorized actions, and potential security violations
- ☐ Utilize security information and event management solutions to compile and analyze app security logs
- ☐ Implement intrusion detection and prevention systems (IDPS) to detect anomalous network traffic
- ☐ Conduct regular vulnerability assessments to identify security flaws