CYBERSECURITY BEST PRACTICES FOR SMALL-SCALE HOSPITALS

Protect patients. Secure data. Strengthen trust.

01 PROTECT ELECTRONIC HEALTH RECORDS (EHRS)

Protect Electronic Health Records (EHRs) through strict access controls and authentication mechanisms.

02 IMPLEMENT ROLE-BASED ACCESS MANAGEMENT

Implement Role-Based Access Management to ensure staff access only information necessary for their responsibilities.

03 SECURE MEDICAL DEVICES AND SYSTEMS

Secure Medical Devices and Systems by maintaining current software versions and security updates.

04 ENCRYPT PATIENT INFORMATION

Encrypt Patient Information to safeguard confidentiality and comply with healthcare regulations.

05 MAINTAIN REGULAR DATA BACKUPS

Maintain Regular Data Backups and verify the integrity of backup and restoration processes.

06 PROVIDE SECURITY AWARENESS TRAINING

Provide Security Awareness Training to clinical and administrative personnel.

07 SEGMENT NETWORKS

Segment Networks to isolate medical systems, administrative systems, and guest internet access.

08 MONITOR AND AUDIT SYSTEM ACTIVITY

Monitor and Audit System Activity to detect unauthorized access and suspicious behavior.

09 ESTABLISH RANSOMWARE PREPAREDNESS

Establish Ransomware Preparedness Measures including backup, recovery, and response procedures.

10 DEVELOP BUSINESS CONTINUITY & INCIDENT RESPONSE PLANS

Develop Business Continuity and Incident Response Plans to ensure uninterrupted patient care during cyber incidents.

STRONG SECURITY. SAFER PATIENT CARE.

Small steps today. Safer hospital tomorrow.