Asset	Asset Value
Patient Medical Records	Very High
Billing Information	High
Employee Records	High
Internal Communications	Medium
Computer systems	Very High
Mobile devices	Medium
Laptops and portable devices for staff	Medium
Servers storing data	Very High
Data backup systems	High
Wireless networks	High
Third-party cloud service providers	Medium
Network infrastructure	High
Website and patient portal	Medium
Electronic prescriptions and healthcare apps	High
Secure communication systems	High
Firewalls and intrusion detection systems	High
Antivirus software and endpoint security tools	High
Data encryption tools	High
HR and payroll software systems	Medium
Healthcare delivery processes	Very High
Patient appointment scheduling systems	High
Employee access credentials	Medium
Legal and compliance	Very High
IT support personnel and system administrators	High
Data storage media	High

Impact of Loss/ Damage to the Asset	Threats to the Asset	Likelihood of Damage
Crucial	Hackers, Ransomware	Medium
Important	Phishing, Hackers	High
Important	Hackers, Thieves	High
Moderate	Phishing, Hackers	Medium
Crucial	Hackers, Malware	Very High
Important	Thieves, Malware	High
Important	Malware, Thieves	High
Crucial	Ransomware, Hackers	Very High
Important	Hackers, Data Corruption	High
Important	Hackers, Unauthorized access	High
Moderate	Unauthorized access, Service outages	Medium
Important	DDoS attacks, unauthorized access	High
Important	DDoS attacks, unauthorized access	Medium
Important	Hackers, Malware	High
Important	Malware, Unauthorized access	High
Important	Hackers, DDoS attacks	High
Important	Maleware, Hackers	High
Important	Unauthorized access, Hackers	High
Moderate	Data breaches, Unauthorized access	Medium
Crucial	Unathorized access, Data breaches	Very High
Moderate	Data breaches, Unauthorized access	High
Moderate	Phishing, Unauthorized access	Medium
Crucial	Data breaches, Unauthorized access	Very High
Important	Unathorized access, Hackers	High
Important	Thieves, Unauthorized Access	High

Justification
Highly sensitive information critical for patient care and highly targeted by attackers
Essential for financial operations, vulnerable to fraud and data breaches
Contains personal information, at risk of identity theft and insider threats
Important for daily operations but less critical compared to medical records
Core infrastructure for all digital activities, prone to various cyber threats
Used for remote work, susceptible to theft and malware
Contain sensitive data, at risk of theft and unauthorized access
Centralized data storage, critical for operations, highly targeted
Ensures data recovery, vulnerable to ransomware and data corruption
Enables connectivity, susceptible to unauthorized access and attacks.
Depend on usage, exposed to cloud-specific security threats.
Backbone of IT operations, targets for DDoS and hacking attempts.
Interface with patients, prone to defacement and denial of service attacks.
Critical for patient care, targets for malware and unauthorized access.
Protects sensitive information exchange, prone to eavesdropping and attacks.
Essential for network security, targets for bypass and configuration attacks.
Protects systems from malware, needs constant updates to remain effective.
Protects data at rest and in transit, vulnerable to key management failures.
Manages employee data, targeted for fraud and unauthorized access.
Core to patient care, highly disruptive if compromised.
Ensures efficient patient flow, prone to unauthorized access and disruptions.
Access control, critical for security, vulnerable to credential theft.
Ensures regulatory compliance, high impact if not maintained.
Maintain IT operations, insider threats and human errors are significant risks.
Stores critical data, prone to theft, data corruption, and unauthorized access.