ID NO.	RISK or HAZARD DESCRIPTION	RESOURCES IMPACTED	EXISTING CONTROL MEASURES	PROBABILITY LEVEL	IMPACT LEVEL	PRIORITY VALUE	PREVENTION MEASURES
Regulaton Requirement							
1	Data Privacy (regulatory non-compliance)	- Financial Loss (fines, legal fees) - Company Reputation (customer trust/loyalty) - Customer Data (PHI and PII)	- Data inventory and calssification - Access control - Data encryption	High	High	9	- Regular audits and security assessments - Data privacy policy - Security awareness training
2	Data Retention and Destruction (regulatory non-compliance)	- Financial Loss (fines, legal fees) - Operational Efficiency	- Data classification	High	High	9	- Data retention policies - Data destruction procedures
Third Party + Cloud							
3	No vender risk management	- Company Reputaion - Data (PHI and PII) - Financial Loss (legal fees, loss of business)	- Contract	High	High	9	- Vender assessment - Monitoring
4	Supply Chain Attack (Vendor Compromise)	- Data (PHI and PII) - Operations - Financial Loss	- Incident response plan - Access control	Medium	High	6	- Monitoring - Stronger incident response plan
5	Supply Chain Discruption	- Data (PHI and PII) - Operations - Financial Loss		Medium	High	6	- Risk assessments - Data redundancy
6	CSP Vulnerabilities (like misconfigurations)	- Data (PHI and PII) - Technology (applications and systems)	- Access controls - Data encryption - CSP contract	Medium	High	6	- Regular vulnerability assessment
7	CSP Breach	- Data (PHI and PII) - Technology (applications and systems) - Company Reputation - Financial Loss	- CSP contract - incident response plan - Regular monitoring	Medium	High	6	- Regular audits - Stronger incident repsonse plan - Business continuity plan - Data backup and recovery procedure
AI							
8	AI Fairness	- Financial Loss (fines, legal fees) - Company Reputation (customer trust/loyalty) - Operational Efficiency	- Transparancy and explainability (disclaimer) - Regular monitoring	Medium	High	6	- Data quality assessment - Regular audits - Human oversight
9	Privacy Violations (AI)	- Regulatory Compliance - Company Repuation (customer trust/loyalty)	- Model testing - Transparancy and explainability (disclaimer)	Medium	High	6	- Regular vulnerability assessment - Data anonymization (remove PII information) - Strong encryption - Strong access control - Input Sanitazion
10	Model Bias (AI)	- Regulatory Compliance - Company Repuation (customer trust/loyalty) - AI Model Accuracy	- Model testing - Transparancy and explainability (disclaimer)	Medium	High	6	- Diverse and representative dataset - Data quality assessment - Human oversight - Regular model monitoring
11	Model Exploitaiton and Manipulation (AI)	- AI Model Accuracy - Company Reputation (customer trust)		Medium	High	6	- Regular model monitoring - Data quality assessment -Input Sanitazion
Asset Management							
12	Lack of Structured Risk Management	- Data (PHI and PII) - Operations - Technology (applications and systems)	- Incident response plan - security controls	Medium	High	6	- Risk management framework - Regular risk assssment - Stringer incident response plan
13	Legacy Applications/Systems	- Data (PHI and PII) - Operations - Company Reputation	- Access controls - Data encryption	Medium	High	6	- Upgrade legacy systems - Regular patching
14	Data Breach	- Financial Loss (fines, legal fees) - Company Reputation (customer trust/loyalty) - Customer Data (PHI and PII)	- Access control - Data encryption - Incident response plan	Medium	High	6	- Strong network security - Security awareness training - stronger incident response plan
15	Data Loss	- Financial Loss (fines, legal fees) - Company Reputation (customer trust/loyalty) - Customer Data (PHI and PII)	- Data encryption	Medium	High	6	- Data redundancy - Disaster recovery plan
Human Interference							
16	Social Eningeering	- Data (PHI and PII) - Technology (applications and systems)	- Access controls	Medium	Medium	4	- Security awareness training

ID NO.	RISK or HAZARD DESCRIPTION	RESOURCES IMPACTED	EXISTING CONTROL MEASURES	PROBABILITY LEVEL	IMPACT LEVEL	PRIORITY VALUE	PREVENTION MEASURES
17	Insider Threat	- Data (PHI and PII) - Technology (applications and systems)	- Access controls - Backgorund checks	Low	High	3	- Security awareness training - Data loss prevention
18	Human Error (like accidental data deletion)	- Data (PHI and PII) - Technology (applications and systems)		Low	Medium	2	- Security awareness training
Physical							
22	Natural Disaster	- Data centers - Technology (network infrastructure, hardware, equipment)	- Insurance - Off site data storage - Physical security	Low	High	3	- Data redundancy - Disaster recovery plan