Mpirik's Security Measure	HIPAA Requirement	HITRUST CSF v9.3	GDPR	Risk Mitigation
Application Controls				
Web Application Firewall	§164.306(a)	10.b	Article 32, Section 1(b)	Application layer flaws and exploit
Network Controls				
Intrusion Detection/ Intrusion Prevention	§164.306(a)	09.m	Article 32, Section 1(b)	Malicioius traffic detection and prevention
Network Firewall	§164.306(a}	01.m, 01.o, 01.w, 09.m	Article 32, Section 1(b)	Unwanter network connectivity
Internal Vulnerability Scanning	§164.308(a)	10.m	Article 32, Section 1(d)	Exploits due to missing patches and updates; improper network firewall configuration
External Vulnerability Scanning	§164.306(a)	10.m	Article 32, Section 1(d)	Exploits due to missing patches and updates; improper network firewall configuration
Two Factor Authentication	§164.312(d), §164.312(a)(2)(iii)	01.j, 05.i, 09.s	Article 32, Section 1(b)	Unauthorized access
TLS 1.2 Encryption in Transit	§164.312(e)(1)	09.m, 09.s	Article 32, Section 1(a)	Interception of sensitive data in transit
Network Segmentation	N/A	08.m	N/A	Reduce the attack surface of unauthorized access or intrusion
Server Controls				
File Integrity Monitoring	§164.312(e)	09.ab, 10.h	Article 32, Section 1(b)	Monitor for unauthorized changes to critical files
OS Patching	§164.306(a)	10.m	Article 32, Section 1(b)	Update for OS weaknesses
Log and Audit Management	§164.308(a)(1)(ii)(d), §164.308(a)(5)(ii)(C), §164.312(b)	09.aa, 09.ab, 09.ac	Article 32, Section 1(b) and 1(d)	Detection of malicious activity
AWS 256 Encryption at Rest	§164.312(e)(1)	09.m, 09.s	Article 32, Section 1(a)	Unauthorized access to sensitive data at rest
Time Synchronization	§164.306(a)	09.h	Article 32, Section 1(b) and 1(d	Forensic analysis
AES 256 Data Encryption at Rest	§164.312(d), §164.312(a)(2)(iii)	06.d, 10.g	Article 32, Section 1(a)	Unauthorized disclosure of sensitive information
End Point Controls				
Endpoint malware protection	§164.308(a)(1)(ii)(D), §164.308(a)(5)(ii)(B), §164.312(b)	Endpoint Protection Domain Vulnerability Management Domain Audit Logging Monitoring Domain	Article 32, Section 1(b)	Antivirus protection and detection of malicious activity on user endpoints
Enterprise endpoint management	§164.308(a)(1)(ii)(D), §164.308(a)(5)(ii)(B), §164.312(b)	Endpoint Protection Domain	Article 32, Section 1(b)	Control of acceptable usage and maintence of user endpoints

Administrative Controls				
Change Control	§164.306(a)	09.g(10)	Security Best Practice	Prevent unauthorized system changes
Risk Assessment	§164.308(a)(1)	03.a, 03.b, 03.c	Artical 32, Section 1	Identification of risks and threats and mitigaction planning
Incident Response	§164.308(a)(6)	05.b, 11.a, 11.c	Artical 32, Section 1(b)	Response to security incidents
Access Control and	§164.312(a)(1)(12)	01.a	Artical 32, Section 1(b)	Prevent unauthorized access
Minimum Necessary Access	§164.502(b), §164.514(d)	1129.v	Article 5, Section 1(c)	Limit access to only required data to complete job function
Continuous Backup	§164.308(a)(7)(ii)(A), §164.310(d)(1), §164.310(d)(2)(iv)	12.c	Article 32, Section 1(b) and 1(c)	Prevent loss or corruption of data and resiliency for disaster recovery
Business Associate Contracts	§164.308(b)(1)	05.k, 09.e	N/A	Legal liability for data loss or breach
Security Audits	§164.308(a)(8)	06.g	Article 32, Section 1(d)	Validation of security controls program
Penetration Testing	§ 164.302 – 318	07.b	N/A	Identify security vulnerabilities