INFORMATION SECURITY PROGRAM OVERVIEW

MedReportGuard's Information Security Program is comprised of the following key components:

Security Philosophy:

• **Defense in Depth** – Multiple, different layers of security are applied across the security domain.

• **Least Privileged Access** – Customers and users are allowed the correct access to achieve the desired business function with only the needed features and information.

• **Role Based Security** – Everyone who has accesses is granted access by role to only the information needed to perform their job function.

• **Encryption** – All restricted data (PII & ePHI) is encrypted in transition and at rest.

• **Limited footprint** – Customer data is limited to the fewest number of high security systems possible.

Hosting Provider / Data Center:

Best in class hosting provider known for their security controls that exceed industry best practices including HIPAA compliance requirements. A sub-set of their security services leveraged by MedReportGuard include:

• IP reputation filtering
• DDoS mitigation
• WAF (Web Application Firewalls)
• IDS (Intrusion Detection System)
• Hardened Hypervisor
• Individual Hypervisor Firewalls
• Anti-virus/Malware Protection
• Hardened Operating Systems
• OS patching
• MFA / Two-Factor Authentication
• Internal and External Vulnerability Scanning

Hosting provider has been validated against the PCI DSS v3.0 and the HITRUST CSF and holds an ISO27001 certification as well as unqualified SSAE 16 SOC 1 and 2 Type II reports.

Software Security:
We leverage a hardened development language to create applications which provides additional security features like:

• PDO parameter binding is used to automatically prevent SQL injection attempts.
• CSRF (Cross-Site Request Forgery) tokens are used and passed along with the form contents to prevent Cross-Site Request Forgery
• Output escaping prevents users from embedding scripts into output, thereby preventing Cross-Site Scripting Vulnerabilities.
• Passwords are Hashed and Salted.
• Role based security restricts users access to only their information that is required to perform their job function. Records are owner and team based.

Encryption:
Strong encryption is deployed using the AES-256 standard for persisted PII and patient medical data. Encryption best practices are also implemented so fields that can contain free form content are encrypted on submission and user profile information is encrypted in the database. Additionally, PII is removed from records when transmitted to the query engine.

Secure encrypted cookies are used with HTTPS for web based access using SSL TLS 2.0