



Exym has served as the EHR platform of many San Bernardino agencies for the past decade with zero breaches. Exym is ONC certified.

Server security: KCare does not have *any* unencrypted PHI, PII, or, any data from or related to our customers in the system at all. All of our servers in all environments are encrypted at rest, and all of our data transfers are encrypted in transit.

Antivirus/malware software: All KCare servers and user endpoints are protected by SentinelOne, an industry leading EDR, backed by a 24/7 SOC monitored by Arete.

Patch management: All systems are patched automatically, as defined in the KCare Vulnerability Management policy. Emergency patches (0 day) must be applied within 7 days. Critical and Important patches must be applied within 30 days.

Transmission encryption: All connectivity to KCare systems is encrypted. A number of different standard are employed, depending on the use case. The primary method of access, HTTPS with TLS, uses SHA256withRSA. You can actually check the specific algorithms we use for this externally at

Qualys: <https://www.ssllabs.com/ssltest/analyze.html?d=sbchc.exym1.com&hideResults=on&latest>

Intrusion detection/prevention: SentinelOne EDR runs on all KCare servers and endpoints. Additionally, our websites are protected by Web Access Firewalls (WAFs) from Cloudflare.

System security review: KCare performs 3rd party reviews annually. This includes both policy and active controls.

Log review: KCare system logs are stored in our SIEM. Both human and Machine learning (ML) reviews of SIEM data are completed.

Change control: KCare has a robust Change Management policy that applies to all systems.