Cloud-Based Solution Checklist

Vendor/Provider

Physical Security

- Are all secure areas are protected by demising walls?
- Are all secure areas use two factor access control (i.e., card swipe and pin)?
- Does provider require a sign in procedure for visitors, service providers, etc.?
- Are all visitors in secure areas must be escorted?

Employee and contractor verification

- Does provider perform criminal background check on employees, contractors, and service providers?

Access and Change Control Audit

- Is provider SSAE 16 SOC2 Type 2 Compliant?
- Name of CPA audit firm performing the SSAE audit?
- Date of last audit?

Vulnerability Assessment

- Date of most recent security vulnerability assessment?

Data Protection

- Where will Missoula County's data be resident?
- Is data encrypted at rest? If so, provide encryption standard in use.
- Please list any security standards provider is certified in, HIPAA, SOX, GLBA, CJIS, PCI, etc.?
- Are all network communications encrypted? If so, provide encryption standard in use.
- Provide an outline of backup procedures.
- Are data backups stored offsite? If so where, and by whom?
- Are data backups encrypted?
- Is the service multi-tenant?
- Is the service segmented on virtual machines?

Business Continuity and Disaster recovery

- Describe plan for power and critical service failure.
- Describe plan for physical disasters such as fire, water, or natural disaster.
- Describe plan for security breaches resulting in failure of core systems, such as DDOS attack.
- Does provider have a DR failover site? If so, does the failover site adhere to the same standards as the primary site?
- Is the failover considered active-active or active-passive?

Network traffic and access logging

- Is provider logging access to the system, switches, databases, routers, firewalls, etc.? If so, would the provider be willing to share the logs upon request?
- Is logging is enabled what is the retention period?

Client connections and authentication

- How are client connections secured?
- Is there support for SSO with Azure and/or ADFS?
- Are strong user passwords required? Please provide password policy.

- Is multifactor authentication required or available?

Service Level Agreement

- Provide SLA information.
- Describe penalties associated with SLA breach.
- Will you accept our BAA, or have a standard BAA (Business Associate Agreement) for HIPAA purposes?

Insurance

- Provide a copy of provider's liability insurance coverage.
- Provide a copy of provider's cyber liability insurance coverage.

Solution Security & Features

Application Requirements

- What are the hardware and OS requirements?
- Any dependent applications (specific browsers, SSMS, etc.)?
- Are there any connectivity requirements (multiple servers, etc.)?
- Are there any required services and permissions (SQL Server service, Server Admin role, etc.)?
- Do you support Microsoft SQL Server, and can the DB be deployed to a shared SQL instance?

Security Requirements

- How is authentication secured? Is it compatible with Active Directory, ADFS, LDAP, or Azure AD?
- Is the application able to utilize multifactor authentication?

Data Protection

- Where will Missoula County's data be resident?
- Are all network communications encrypted? If so, provide encryption standard in use.