

Are there any alternatives or backup facilities for the services provided by this Service Provider?

Yes, alternates for critical services

Yes, alternates for all services

No

During the last 12 months, how many significant outages have the Service Provider experienced?

1. Several (>5)

2. Many (3-5)

4. None

3. Moderate (<3)

How might patients be affected by downtime of this Service Provider?

Downtime could inconvenience patients

Downtime could delay patient treatment

Downtime could result in aggravated patient condition

Downtime would not affect patients

What services/functions does the Service Provider provide? -- (selection is required)

Supply Chain Services/Management

Business - Critical ASP Service

Customer Care Services

Back office Transaction Processing

Has the Service Provider ever filed for Bankruptcy? -- (selection is required)

Yes, but is now fiscally sound

Yes

No

What volume of ePHI is Stored, Processed, or Transmitted by/with this Service Provider? -- (selection is required)

Low volume of ePHI (<100 records)

No ePHI

High volume of ePHI (>200 records)

Medium volume of ePHI (100-200 records)

Service Provider - all controls

Does the InfoSec policy include a physical access policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include a security awareness & training policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Access to any systems are limited to administrators only. All access is monitored.

Does the InfoSec policy include an acceptable use policy (restriction on using organization resources for purposes outside of business)?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include a policy for assigning and managing file directory permissions?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include an Internet & Intranet access / use policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include an encryption policy and encryption standards policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include an email use policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include a policy for minimum security configuration standards (networks, operating systems, applications and desktops)?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include a password policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include a version control policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include an anti-virus & malware protection policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include a network security & access policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include a remote access policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include an SDLC policy for application development and supporting infra-structure?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include a change management policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include an incident management & response policy?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the InfoSec policy include disaster recovery and business continuity plans?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Has the InfoSec policy been published & is it easily accessible to all members of the workforces?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

How often is the InfoSec policy reviewed?

Reviews are not conducted -- (You may enter comments below)

Ad hoc -- (required comment: When was the last occurrence?)

Occurs > 24 months -- (required comment: When was the last occurrence?)

Occurs < 24 months -- (required comment: When was the last occurrence?)

January 2006

Occurs < 12 months -- (required comment: When was the last occurrence?)

Occurs < 6 months -- (required comment: When was the last occurrence?)

N/A -- (You may enter comments below)

Does the policy reviewer have appropriate skills & experience to conduct the review?

No -- (You may enter comments below)

Not reviewed by a security policy specialist or expert -- (You may enter comments below)

Reviewed by a security policy specialist or expert -- (required comment: Summarize the qualifications of the reviewer)

N/A -- (You may enter comments below)

Are all of the services provided to the Client (BHCS) internally hosted & maintained vs outsourced?

No

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (required comment: What services are outsourced?)

N/A -- (You may enter comments below)

Is a risk assessment conducted to evaluate types of access provided to the Technical Service Providers?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Are protections in place to ensure that the Technical Service Provider are provided the appropriate level of physical access according to their business need?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Is the Technical Service Provider who access information processing systems covered by formal contracts referencing the security requirements?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Are verification (background) investigations conducted on applicants for permanent employment?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Do the background inquiries check the availability of at least one satisfactory business & personal character reference?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Is a physical security program in place for protecting the business premises & information processing systems from damage, interference & unauthorized access?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Is there a physical security plan which includes physical barriers around the premises & information processing systems?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Is all server equipment related to the Client's services located in a computer room / data center?

No -- (required comment: Where is server equipment located besides data-centers?)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Do the service provider's computer rooms/data centers have temperature and humidity control systems that are separate from the rest of the facility?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Service Provider - all controls (cont)

Are the computer room / data centers temperature and humidity systems actively monitored and alarmed during off-hours?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Do the computer rooms / data centers have fire suppression systems and water detection systems?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Do the computer rooms / data centers have fire extinguishers?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Is all of the equipment related to the Client's (BHCS) service located and maintained on-site (vs. off-site, external hosting)?

No -- (required comment: Where is the equipment located?)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Servers are co-located in Phoenix Az.

Are safeguards in place to ensure a continual and regulated supply of power for equipment?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Are uninterruptible power supplies (UPS) in place to protect equipment from power failures?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Are generators in place to protect equipment from power failures?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Are backup generators used in cases where processing must continue during long power outages?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the Service Provider separate its development, test & production (operational) environments?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (required comment: Describe how this separation is accomplished)

N/A -- (You may enter comments below)

Testing development is done on different servers

Does development, testing & operational software run on different computer processors, in different domains and/or directories?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the Service Provider monitor current & future capacity demands to ensure that adequate processing

Institutional Risk Assessment of Vendors

power & storage are available?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Have controls been implemented to detect & prevent malicious software?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

How often are desktop & server virus definitions updated?

No updates

Ad hoc updates

Monthly updates

Weekly updates

Daily updates

N/A

Are regular back-ups performed for systems and data relating to the Client?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

How often are back-up copies of essential business-critical information made?

Backups are not conducted -- (You may enter comments below)

Ad hoc -- (required comment: When was the last occurrence?)

Occurs > 3 months -- (required comment: When was the last occurrence?)

Occurs < 1 month -- (required comment: When was the last occurrence?)

Occurs <1 week -- (You may enter comments below)

Occurs daily -- (You may enter comments below) every 15 minutes

N/A -- (You may enter comments below)

How often are restoration procedures tested to ensure they can be completed within the time allotted in the operational procedures for recovery?

No testing

Ad hoc -- (required comment: When was the last occurrence?)

Occurs > 24 months -- (required comment: When was the last occurrence?)

Occurs < 24 months -- (required comment: When was the last occurrence?)

Occurs < 12 months -- (required comment: When was the last occurrence?)

January 2006

Occurs < 6 months -- (required comment: When was the last occurrence?)

N/A -- (You may enter comments below)

Does the Service provider log and monitor firewall activity?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (optional comment: Describe how firewalls are monitored)

N/A -- (You may enter comments below)

Are allocation and use of system administrative privileges restricted and controlled?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

S9.3.2.1> What is the minimum password length for standard system Users?

Institutional Risk Assessment of Vendors

No minimum password requirements -- (You may enter comments below)

< 6 character minimum -- (You may enter comments below)

6 character minimum -- (You may enter comments below)

7 character minimum -- (You may enter comments below)

8 character minimum -- (You may enter comments below)

> 8 character minimum -- (You may enter comments below)

N/A -- (You may enter comments below)

Password minimums and security rules are defined by system administrator to match requirements of organization

Are restrictions on connection times required for critical applications?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the Service Provider employ the use of encryption for the protection of sensitive or critical information?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Is the Client's sensitive data encrypted on all networks within the Service Provider that transmit & receive such data?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (required comment: What type and bit-level of encryption is used?)SSL 128 bit

N/A -- (You may enter comments below)

Is the Client's sensitive data encrypted on all systems within the Service Provider that store such data?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Only passwords and SSN are encrypted at the DB level

Yes -- (required comment: What type and bit-level of encryption is used?)

N/A -- (You may enter comments below)

Does the Service Provider employ the use of digital signatures?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Does the Service Provider avoid using operational databases containing personal information for testing?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

S10.8.1.2> Does the Service Provider require depersonalization of such information, if it must be used?

No -- (You may enter comments below)

Yes, but with exceptions -- (required comment: What exception(s) exist?)

Yes -- (You may enter comments below)

N/A -- (You may enter comments below)

Are all areas within the Service Provider subject to regular review to ensure compliance with security policies & standards?

Reviews are not conducted

Ad hoc -- (required comment: When was the last occurrence?)

Occurs > 24 months -- (required comment: When was the last occurrence?)

Occurs < 24 months -- (required comment: When was the last occurrence?)

Occurs < 12 months -- (required comment: When was the last occurrence?)

July 2006

Occurs < 6 months -- (required comment: When was the last occurrence?)

N/A -- (You may enter comments below)

How often are information systems checked for compliance with security implementation standards?

Reviews are not conducted

Ad hoc -- (required comment: When was the last occurrence?)

Occurs > 24 months -- (required comment: When was the last occurrence?)

Occurs < 24 months -- (required comment: When was the last occurrence?)

Occurs < 12 months -- (required comment: When was the last occurrence?)

July 2006

Occurs < 6 months -- (required comment: When was the last occurrence?)

N/A -- (You may enter comments below)