Vendor Security Questionnaire

Business Associate

Vendor Name

Vendor URL

Vendor Contact

Address

Vendor Contact Email Address

Vendor Contact Phone Number

What type of Service do You Provide Covenant Health?

How is Protected Health Information (PHI):

Used

Accessed

Stored

Has a Network Penetration Test be Done on Website (applicable if using a web-based product)

Has a Application Penetration Test be Done on Website (applicable if using a web-based product)

Administrative Safeguards

Do you keep an inventory of where Protected Health Information (PHI) is:

Used

Disclosed

Stored

Transmitted

When was the last Security Risk Analysis Conducted?

When was the last Compliance Assessment Evaluation Conducted?

Vendor Security Questionnaire

Is ePHI Stored or Accessed on Portable Media?

If YES Describe your Security Measures? (Attach Policy)

What was the Date of Your Last Full Backup?

Describe the Process or Attach the Policy and/or Form to Grant Workforce Members Access.

Describe or Attach all Security Testing that has been Performed over the Past Year. Have you been Audited against any of the following Guidelines or are you Currently certified against any of the following standards?

NIST, HIPAA, PCI DSS, ISO 27001, ISO 27002, SSAE16 SOC1 or SOC2, ISAE3402, CSA

Cloud Controls Matrix, or other equivalent standard?

Are you able to share with us a current report of the audit results?

Physical Safeguards

Describe your Measures to Destroy Items Containing PHI (Media, Paper, Hard Drives).

Is there a Disaster Recovery Program and Back-up Process?

Where is (are) your data center(s) located?

Describe the physical security, disaster recovery, back up/redundancy, and prevention features of your data center.

Who (including data center staff, other employees and vendors) has physical access to the host servers?

Vendor Security Questionnaire

Network Security

Are industry-standard firewalls deployed? Where are they deployed? Is the software and firmware on the firewall at a supportable level? Is administrative access to firewalls and other perimeter devices allowed only through secure methods?

Does your company use an intrusion prevention system OPS?

Does your company use intrusion detection systems (IDSs)? How long are IDS logs kept?

Are formal incident-response procedures in place? Are they tested regularly?

How are operating systems kept up to date?

How does your company keep abreast of software vulnerabilities?

What Is the procedure for installing software updates?

Are file permissions set on a need-to-access basis?

Are ongoing vulnerability assessments performed against the systems?

Vendor Security Questionnaire

System Security

Are ongoing vulnerability assessments performed against the systems?

Are audit logs implemented on all systems that store or process critical information? How often are these logs reviewed?

Staff Security

Has the staff undergone complete background and criminal checks?

What are the on call processes for security staff?

Are screen-blanking mechanisms deployed on all employee workstations?

Do sessions automatically time out after an idle period?

Describe the user account and password policy.

Security Breach Response

Describe your security breach response policies.

Have you experienced any security breaches in the past 36 months?

Describe your anti-virus strategy including the products you use.

Vendor Security Questionnaire

Disaster Recovery/Back Up

Describe your disaster recovery/back up policy.

How often is your disaster recovery plan updated?

Has your disaster recovery plan been tested?

Privacy/Confidentiality of Data

How does your company protect the privacy of any information that may be collected and maintained through the software?

Are your data centers SSAE16 audited and/or is your operating environment ISO 27001/27002 compliant?

How is data integrity ensured?

What checks are carried out on people who might have access to the data?

Transition Services

What happens to our data if we decide to terminate the license/subscription with your company?