Goshen Health

Dear Vendor:

Goshen Health requires that vendors that are hosting\storing\transmitting our business data demonstrate compliance with the HIPAA Security regulations or to demonstrate that they have a strong information security program implemented if they are not storing protected health information (PHI), but other confidential business data. This validation includes any of your subcontractors that handle our business data.

Your organization and your subcontractors who handle or access our business data must submit documented evidence that they meet the HIPAA Security Rule, including the information security risk assessment and management requirements defined in the regulations or an information security framework certification for those not hosting PHI. Evidence of your compliance program includes any results of your information security risk assessment, certification, or audit, including the status of any issues that were identified as not meeting the requirements. The goal is to ensure that your organization as well as each of your subcontractors meets information security requirements (administrative, technical, and physical controls), these controls are included in your information security program, and the security controls established and audited regularly. Evidence must be submitted for your organization and also for any of your subcontractors involved in the handling or hosting of our data.

If you are handling or hosting PHI, the following web sites are provided by the Department of Health and Human Services and can be a reference to you or your subcontractors regarding these requirements:

OCR Security Rule Guidance:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Guidance on Risk Analysis Requirements under the HIPAA Rule:
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

OCR Protocol for HIPAA Audit Program:
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol2.html

Acceptable evidence of an information security program can be provided using one of the following documents:

- SSAE16 (SOC2 or 3) or ISO 27000 series audit report conducted by a qualified third party
- HITRUST Certification
- NIST SP 800-66 – Guide for Implementing the HIPAA Security Rule
- Information Security Risk Assessment performed by internal certified information systems security professionals (the assessment, the results of the assessment, and status of remediation of findings)
- Other information security certifications or framework audits that cover equivalent information security controls outlined in the HIPAA Security Rule.

If your organization or your subcontractors are unable to meet these requirements we will not proceed with off-site hosting. If available, we may alternatively look to host the system or software through the Goshen Health Information Technology Services Department.