Gruppo Marcucci, LLC - - SECURITY REVIEW QUESTIONS

Please provide the following documents:
1. Overview of data center infrastructure
2. Network and System infrastructure diagrams
3. System dataflow / integration diagrams
4. Business Continuity and Disaster Recovery plans
5. Security, privacy policies and procedures
6. IT/Security Personnel Organization Chart

1. Systems & Technology Audits	
	Describe all audits, tests & reviews conducted over the past 24 months internally or by clients, prospects & 3rd party vendors that you have hired specifically for audit purposes.
Question 1a.	a. Your **OPERATIONS** audits: • SSAE 16 (SOC 1, SOC 2, or SOC 3) (Include Issue Date, Type and Opinion) (If you have not yet conducted a SSAE 16 SOC audit, explain plans in place and timing of doing so)
Question 1b.	b. Your **DATA CENTER** audit: • SSAE 16 (SOC 1, SOC 2, or SOC 3) (Include Issue Date, Type, and Opinion Type) (If you have not yet conducted a SSAE 16 SOC audit, explain plans in place and timing of doing so)
Question 1c.	c. Security and Technical audits, tests and reviews including the following (be sure to list internal or external and if external performed by whom) • IT Risk Assessment Audit (ISO 2700 standard) • Application Code Reviews • Penetration or Vulnerability Scans • Security Audits

2. Security	
	Provide the following information:
Question 2a.	a. Have you ever been required to disclose a HIPAA breach of information for a client's EE population? If yes, what steps were taken to resolve? If yes, was your breach 1) Unintentional (Stolen Laptop), 2) Intentional (Disgruntled Employee), or 3) Outside Breach? Do you have a data breach plan in place?
Question 2b.	b. Has your company been under examination by the Department of Labor (DOL) or Department of Health and Human Services (HHS) within the last 4 years in relation to HIPAA security or procedures? If so, was remedial action required and/or were fines assessed in relation to service failures affecting your current or former clients?
Question 2c.	c. Describe your process for storing client data (i.e., servers, locations, cloud, etc.). What redundancy and security processes are used to ensure continuity of service?
Question 2d.	d. Confirm compliance with all HIPAA & HITECH requirements and regulations. Confirm you have a dedicated department and/or dedicated staff members responsible for monitoring and assuring HIPAA compliance.
Question 2e.	e. Confirm all subcontractors' compliance with all HIPAA & HITECH requirements and regulations. Confirm you will be responsible for executing BAA's with subcontractors and will be responsible for any subcontractor breaches in data security.

3. Encryption			
	Provide the following information:		
Question 3a-f.	Description of your encryption protocol?		
		Encrypted (Yes/No)	Additional Details
	a. Level: Database		
	b. Level: Field		
	c. In Transit		
	d. Internal to your network		
	e. External to your network		
	f. Back-Up Data		
Question 3g.	g. Who has control over the decryption keys?		
Question 3h.	h. Do you use 256-bit encryption for web interaction?		
Question 3i.	i. Are your data files encrypted during transmission? (i.e. SFTP)		
Question 3j.	j. How is it protected at the destination?		
Question 3k.	k. Outline the "front door" protection (i.e. protected using ID's and Passwords).		
Question 3l-n.	Password protocols.		
	l. Length?		
	m. Construct?		
	n. Duration?		

4. Other	
	Provide the following information:
Question 4a.	a. Your firewall and intrusion protections, network and host based.
Question 4b.	b. Your user authentication process and restrictions.
Question 4c.	c. Your network access policy/approach as it relates to external interfaces.
Question 4h	d. What operating systems (including mobile devices) and browsers are supported?