Questions to Consider

Related to the Safeguards Rule

(16 CFR 314)

Who has the Company designated to coordinate the information security program?
(Safeguards Rule 314.4 (a))

Has an information security risk assessment identifying reasonably foreseeable internal and external information security risks been conducted?
(Safeguards Rule 314.4 (b))

Are safeguards in place to control the risks identified in the risk assessment? And are these safeguards monitored/tested for effectiveness?
(Safeguards Rule 314.4 (c))

How are service providers selected and monitored?
(Safeguards Rule 314.4 (d))

Is the information security program evaluated and adjusted?
(Safeguards Rule 314.4 (e))

Questions to Consider
Regarding Best Practices

#	Question	Company Response	Best Practices and Resources
1	How does the Company assess information security / cyber security risks to the organization? Does the Company follow a documented Risk Assessment Process, including: o Asset Identification o Risk Identification o Risk Assessment and Measurement (analyzing the likelihood / impact on specific assets) o Risk Mitigation (identifying and prioritizing ways to reduce identified risks, describing how identified risks will be mitigated or accepted) o Risk Monitoring		In order to implement information security safeguards, risks to security, confidentiality, and integrity must first be identified. Both internal and external risks to an organization should be considered. For more information regarding the importance of conducting an information security risk assessment, visit the following websites: o Complying with the Safeguards Rule (FTC) o Guide for Conducting Risk Assessments (NIST) o IT Risk Management (FFIEC)
2	Is there an Information Security Incident Response Plan in place? Is a Communication Plan included to notify employees, third party service providers, regulators, and customers, as applicable?		Like physical disasters, computer incidents can occur without warning. It is important to have an Information Security Incident Response Plan in place so that your Company is prepared. Components of an Incident Response Plan might include responsibilities and decision-making authority for designated teams and/or staff members and a communication plan for notifying employees, third party service providers, and regulators, as applicable. Also included should be a plan for notifying customers if a breach has occurred (in accordance with RCW 19.255.010). For more information regarding the importance of implementing an Information Security Incident Response Plan, visit the following websites: o Complying with the Safeguards Rule (FTC) o Data Breach Response – A Guide for Business (FTC)
3	How does the Company back-		Information that is critical to running the

	up data in order to allow the recovery of important documents in the event of a physical disaster or a technical incident?		business should be backed-up regularly and stored securely so that the confidentiality, integrity, and availability of the information is maintained. Backing-up data allows the Company to recover important documents in the event of a physical disaster or a technical incident. For more information regarding the importance of backing-up data, visit the following websites: o Complying with the Safeguards Rule (FTC) o Small Business Information Security: The Fundamentals (NIST; section 3.5, page 25)
4	What password policies are in place for users? Is length, complexity, reuse, and aging considered? Is multi-factor authentication used?		To control access to information, ensure that strong passwords are used. For more information regarding the importance of strong passwords, visit the following website: o Small Business Information Security: The Fundamentals (NIST; section 4, page 31)
5	Is user access limited to business need?		Access to information should be limited to those employees with legitimate business need. For more information regarding the importance of limiting access, visit the following websites: o Complying with the Safeguards Rule (FTC) o Small Business Information Security: The Fundamentals (NIST; section 3.2, page 18) o Cyber Security Planning Guide (FCC; pages 3, 6, and 25)
6	How does the Company ensure all operating systems and applications are patched and updated regularly?		It is important to update and patch regularly so known vulnerabilities can be resolved. For more information regarding the importance of regularly patching and updating, visit the following website: o Complying with the Safeguards Rule (FTC) o Small Business Information Security: The Fundamentals (NIST; section 3.2, page 19) o Cyber Security Planning Guide (FCC; page 12)
7	Are hardware and software		Firewalls inspect and restrict data packets,

	firewalls installed and activated?		allowing only authorized packets through. A software firewall may be included with your operating system. Hardware firewalls may be a function of your router. For more information regarding the importance of firewalls, visit the following websites: o Complying with the Safeguards Rule (FTC) o Small Business Information Security: The Fundamentals (NIST; section 3.2, page 19) o Protecting Personal Information: A Guide for Business (FTC; page 17)
8	Is anti-malware in place on all devices, including employees' personal devices, if used for business purposes?		Anti-malware software is designed to detect and block malware before it causes harm. For more information regarding the importance of anti-virus software, visit the following websites: o Complying with the Safeguards Rule (FTC) o Cyber Security Planning Guide (FCC; pages 9, 10, and 39) o Small Business Information Security: The Fundamentals (NIST; section 3.3, page 23)
9	If Wi-Fi is used, what form of encryption is configured?		If the Company uses wireless internet, ensure that WPA2 level encryption is used. WPA2 is currently the strongest level of wireless encryption. For more information regarding the importance of wireless security, visit the following websites: o Securing Your Wireless Network (FTC) o Small Business Information Security: The Fundamentals (NIST; section 3.2, page 20)
10	How is sensitive information sent from the Company to consumers? How is sensitive information sent from consumers to the Company? Are all electronic transmissions sent securely?		Sensitive information should be sent through encrypted e-mail or a secure portal. Non-encrypted email is not a secure method of transporting sensitive information. Encryption converts the data into an unreadable format so that eavesdroppers cannot easily read the data being transmitted. For more information regarding the importance of sending information securely, visit the following websites:

			o Complying with the Safeguards Rule (FTC) o Small Business Information Security: The Fundamentals (NIST; section 3.2, page 21) o Cyber Security Planning Guide (FCC; pages 19 and 25)
11	How are sensitive paper documents disposed of?		When disposing of paper, ensure that sensitive data is destroyed in such a way that the information cannot be read or reconstructed. For more information regarding the importance of data disposal, visit the following websites: o Complying with the Safeguards Rule (FTC) o Small Business Information Security: The Fundamentals (NIST; section 3.2, page 21) o Cyber Security Planning Guide (FCC; pages 28)
12	How is electronic data (such as hard drives, usb drives, cds, etc.) disposed of?		When disposing of hard drives, mobile devices, or any other electronic media or hardware containing sensitive information, ensure that sensitive data is physically destroyed or erased in such a way that the information cannot be read or reconstructed. For more information regarding the importance of secure electronic data disposal, visit the following websites: o Complying with the Safeguards Rule (FTC) o Small Business Information Security: The Fundamentals (NIST; section 3.2, page 21) o Cyber Security Planning Guide (FCC; pages 28)
13	Is a Clean Desk Policy* implemented? * The purpose of a clean desk policy is to ensure sensitive information is not left unattended.		The purpose of a Clean Desk Policy is to ensure sensitive information is not left unattended. Employees should be expected to lock computer screens and securely store paper documents and mobile devices containing sensitive information when they are away from their desk. For more information regarding the importance of implementing a Clean Desk Policy, visit the following website: o Cyber Security Planning Guide (FCC; pages 25)

Scenarios to Consider

#	Scenario	Defense How does your company defend against this scenario?	Response How would your company respond to the scenario if the incident occurred?
1	**An employee (or vendor) does not dispose of data properly or loses sensitive information (either electronic or on paper).**		
2	**An employee (or vendor) sends data to incorrect consumer.**		
3	**An employee (or vendor) steals consumer information for leads (either for self or to sell).**		
4	**Social engineering tactics are used against employees to gain access to systems or directly gain sensitive information.** **Social engineering tactics include: phishing, vishing (voice phishing), and tailgating (entering secure areas by following closely behind someone else).**		
5	**Someone outside of the organization physically steals items (electronic devices or paper documents) containing sensitive information.**		
6	**Someone outside of the organization electronically steals sensitive information.**		