



Privacy and Security Questionnaire for Service Provider to ABC Company

Please check "yes" or "no" as applicable to whether you are doing or have done the tasks listed below.

Employee Management and Training	Yes	No
1. Check references prior to hiring employees who will have access to nonpublic personal information ("NPI") (NPI means personally identifiable, nonpublic financial and health information, whether maintained in paper, electronic or other form).		
2. Have written security policies and standards that prescribe how employees are to handle NPI.		
3. Require employees to sign an agreement to abide by those security policies and standards.		
4. Train employees on how to maintain the confidentiality, availability, and integrity of NPI.		
<i>For example, train employees to:</i>		
- lock rooms and file cabinets where paper records are kept.		
- use password-controlled screensavers.		
- use strong passwords (at least eight characters long; no actual words).		
- change passwords periodically, and avoid posting passwords near employees' computers or otherwise in plain view.		
- recognize fraudulent or improper attempts to obtain NPI and report it to appropriate company security officials.		
5. Remind employees periodically of company's security policies and to keep NPI secure and confidential.		
6. Limit access to NPI to employees who have a business reason for seeing it.		
7. Impose and document disciplinary measures on employees for failure to adhere to your company's security policies and standards.		
8. Auditing employee and vendor compliance with company's security policies and standards.		

Data Storage and Information Systems	Yes	No
9. Store NPI in a secure area and make sure only authorized employees have access to the area.		
<i>For example:</i>		
- store paper records in a room, cabinet, or other container that is locked when unattended.		
- ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods.		
- store NPI on a secure server		
• is that server password protected.		
• does the server have other security protections.		
• is the server kept in a physically locked and secure area.		
- prohibit storing NPI on a PDA or smart phone with an Internet connection.		
- maintain secure backup media.		
- keep archived data secure; for example, by storing it off-line or in a physically-secure area.		
10. Provide for secure data transmission when you collect or transmit NPI.		
<i>For example:</i>		
- if collect credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection so that the information is encrypted in transit.		
- if collect information directly from consumers, make secure transmission automatic.		
- if transmit NPI by electronic mail, ensure that such messages are password protected so that only authorized employees have access.		
11. Dispose of NPI in a secure manner.		
<i>For example:</i>		
- hire or designate a records retention manager to supervise the disposal of records containing NPI.		
- shred paper NPI.		
- recycle paper NPI and store it in a secure area until a recycling service picks it up.		
- erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contains NPI.		
- remove NPI from reusable hardware.		
12. Maintain an inventory of your computers, other hardware, and software applications.		
13. Monitor manufacturer communications regarding operating systems, application software and hardware vulnerabilities and install patches in accordance with the manufacturer's recommendations.		
14. Use monitoring tools at firewalls and on PCs that alert you if malicious code is present.		
15. Have installed anti-virus software on all of your computers and networks and does it apply updates automatically.		
16. Conduct periodic penetration and vulnerability tests of your company's network and computers.		
17. Have a written contingency plan that addresses breaches of physical, administrative or technical safeguards.		
18. Have an Incident Response Team with tested and documented procedures.		

NPI Availability	Yes	No
19. Document and test procedures to address data backup and recovery (“DBAR”) and business continuity planning (“BCP”).		
20. Include controls in DBAR and BCP plans to preserve the security, confidentiality and integrity of NPI in the event of a computer or other technological failure.		
21. Backup all NPI regularly.		
22. Have audit methods in place to capture system events such as system access, network access, and application access.		

Subcontractors	Yes	No
23. Assign work related to ABC Company to related subcontractors. If no, go to question 26.		
24. Apply same NPI protections to domestic subcontractors, both for work performed/data stored at sites and at the domestic subcontractors’ sites, and audit these protections on a regular basis.		
25. Monitor and close all data connections and access pathways with domestic subcontractors when no longer required.		
Foreign subsidiaries, units, and subcontractors		
26. Perform all work done for ABC Company in locations within the United States by either subsidiaries, affiliates, or units of company or by subcontractors.		
27. Use additional controls and protections for foreign locations.		
<i>For example:</i>		
- Deploy technology that separates the foreign subcontractor/subdivision’s network and company’s network.		
- Encrypt all data in transit between networks when necessary.		
- Use design access methods such as Metaframe or Terminal Services in order to prevent data from being removed from your network.		
- Limit access to internal systems to the minimum necessary.		
- Require unique access ID’s and passwords.		
- Track all cross-border access to NPI.		
28. Monitor and close data connections with foreign subcontractors/ subdivisions when no longer required.		

Important Note: In any case where you have responded “No” to a question, please insert or attach an explanation.