



Privacy questionnaire

1. a. Do you collect, store or transmit payment card information through the internet or through a website? Yes No
b. If so, approximately how many PCI records?
0-1,000 1,000 – 100,000 100,000 – 1m 1m+
c. Do you otherwise collect, store or transmit PCI e.g. offline? Yes No
d. If so, approximately how many PCI records?
0-1,000 1,000 – 100,000 100,000 – 1m 1m+

2. a. Do you collect, store or transmit personal health information? Yes No
b. If so, approximately how many PHI records?
0-1,000 1,000 – 100,000 100,000 – 1m 1m+

3. Please confirm the most private and/or confidential information you hold:

4. How do you store, secure and transmit information securely?

5. Have you specifically mapped the flow of personal/confidential data through your systems? Yes No

6. Who (if anyone) can access data in its unencrypted format?

7. If you are NOT encrypting personal/sensitive data residing in your systems (i.e. data at rest in the database and storage) please describe what you believe are the 'compensating controls' to ensure protection of same:

8. Which third-parties have access to this data?

Privacy questionnaire

9. Outline how you go about risk managing the security and privacy procedures of your business partners:

10. Outline any privacy related projects conducted in the last 12 months and any that are anticipated in the next 12 months:

11. Who regulates your privacy matters? Please outline the level of contact you have with them (including any subpoenas or investigations):

12. Have you made any material changes to your privacy procedures or policy in the last 12 months?

Yes No

Do you plan to do so in the next 12 months?

Yes No

13. Outline how you have, or would, communicate a material change to your privacy practices:

14. Do you have a written procedure setting out how someone should contact you in the event of a privacy complaint?

Yes No

15. Do you also have a written procedure for communicating a privacy breach to state authorities and affected parties?

Yes No

16. Please supply a copy of any recent security audit/assessment your organization has undertaken.



Privacy questionnaire

17. Do you store credit card details on your network or does it go straight off to the payment processor?

18. Have you specifically checked that your SQL servers with credit card details are programmed to prevent SQL injection attacks? Yes No

19. Is your credit card data on your SQL server always encrypted? Yes No

20. Is all Personally Identifiable Information (PII) encrypted at rest and in transit? Yes No

21. Is all Personally Identifiable Information (PII) encrypted on the network and off the network including remote devices, i.e. laptops, blackberries, disks, etc. Yes No

22. Are all back up tapes / cassettes secure in transit? Are they picked up, shipped, and stored by reputable third parties?