

Appendix GG

CONTROLS FOR HANDLING DATA PRIVACY ISSUES

1. Has your organization defined how you assure the fair use of information?
2. Has the organization defined and formalized (in writing) the organization's information handling policies?
3. If you are outsourcing any processes, do all personnel understand them and their risks thoroughly?
4. Are privacy policies in place? Is the company following them? How can you verify this?
5. Are specific individuals assigned to ensuring that privacy policies and procedures are in place and followed? Do their job descriptions confirm that they have these responsibilities?
6. Does your organization provide customers with a clear and conspicuous notice of their information gathering practices, including what personnel information is collected, how it is collected and how the organization plans on using the data?
7. Are systems designed to collect only the amount of individual and household data necessary to perform a specified set of tasks?
8. Are appropriate security measures, methods and techniques in place to protect personal data?
9. Do organizational systems offer Web site users the ability to "opt-out" if having their personal information collected, retained (warehoused), shared and/or used?
10. Are systems designed to give individual users "reasonable access" to personal data and give them the opportunity to correct or delete incorrect information?
11. How is data handled once it enters the organizations internal facility?
12. How is access to data limited and controlled?
13. Are there procedures in place to analyze data and to categorize said data for user access, on a need-to-know basis?
14. What procedures are in place to verify and ensure that all partners, subsidiaries, and third parties that work with, interact with, or receive your organization's data

are themselves compliant with the appropriate and prevailing legislation (i.e., HIPAA, GLB, etc.)?

15. What proactive, ongoing education programs has your organization developed to communicate (on a continual basis) the specifics of appropriate and related legislation and the impact of failing to comply, to all levels of personnel with the organization?
16. Does your organization employ content-filtering software that checks out-going e-mails to ensure details are encrypted where appropriate?
17. Does the organization utilize software that will automatically close patient records and other sensitive on-screen data if there is no activity for a prescribed length of time?
18. Can the organization demonstrate a standard of due care (e.g., does it deploy firewalls, intrusion detection, log-file monitoring, and data encryption) in the propagation of privacy throughout the organization?
19. Does your organization's privacy policy reflect how information is really handled in your company?