

FAQs About Privacy and Security



The Health Insurance Portability and
Accountability Act

HIPAA Privacy Rule Compliance Date: April 14, 2003

1. Does MedQuist have policies and procedures for ensuring the privacy of its clients' Protected Health Information (PHI)?

Yes, MedQuist has written policies and procedures regarding the privacy and confidentiality of patient information.

2. Do MedQuist's policies regarding PHI include remedies for violations (i.e., disciplinary measures)?

MedQuist's confidentiality policies have been rewritten to strengthen the language as well as the associated remedies.

3. Does MedQuist require appropriate approvals before the release of client PHI, and does the release of PHI undergo an audit process?

MedQuist is not designated as the custodian of medical records and does not keep original PHI. All requests for information are referred directly to the client.

4. Are MedQuist clients notified when their PHI has been disclosed to another party?

MedQuist does not disclose any information to third parties. All requests for information are referred directly to the client.

5. How is MedQuist assisting clients in finalizing the required Business Associate Agreements?

MedQuist has developed a Business Associate Agreement to help clients facilitate the process of finalizing agreements. It can be obtained from our Corporate Contracts Department or through your account contact at MedQuist.

6. Does MedQuist have a formal privacy awareness, education and training program available to its workforce?

MedQuist is in the last stages of finalizing the rollout of initial privacy training, new member orientation training, and annual in-service for the entire workforce.



**HIPAA Security Rule Compliance Date:
April 21, 2005**

1. Has MedQuist conducted a formal assessment of the sensitivity, vulnerability, and security of its programs and the client PHI it receives, manipulates, stores, reports and/or transmits?

Yes, MedQuist is continuing to conduct an extensive risk analysis and assessment relating to these issues. We retained a national consulting firm to assist in the assessment, gap analysis and HIPAA strategy development.

2. Has MedQuist conducted a technical and non-technical evaluation of the implemented security standards?

MedQuist will perform a periodic evaluation of its security practices as part of its Corporate Compliance Program. MedQuist anticipates readiness by the compliance date.

3. Are MedQuist employees subject to documented clearance policies and procedures regarding their access to client PHI?

MedQuist is developing security policies related to workforce clearance and access, and anticipates readiness by the compliance date.

4. Does MedQuist have a contingency plan for systems used to process or manipulate client PHI, encompassing all of the following: application data criticality analysis, data backup plan, disaster recovery plan, emergency mode operation plan, and testing and revision procedures?

MedQuist has developed a Business Contingency Plan.

5. Does MedQuist maintain a record of access authorizations to client PHI?

Procedures are being developed and/or enhanced for logging access authorizations to client PHI. MedQuist anticipates readiness by the compliance date.

6. Does MedQuist maintain and review audit logs of system activity reflecting the processing, sharing, transmitting or reporting of client PHI?

MedQuist maintains system activity logs, and current review procedures are being enhanced.

7. Does MedQuist have a security policy that documents procedures for ensuring the prevention, detection, containment, and correction of security issues, and that outlines appropriate sanctions in the event of security breaches?

MedQuist is in the process of creating a written security policy that addresses these issues. We anticipate readiness by the compliance date.

- 8. Does MedQuist protect the systems it uses to process client PHI against computer viruses, including virus-checking new software and educating users about virus prevention? Are MedQuist's policies and procedures documented?**

MedQuist protects its systems against viruses by installing and enabling virus software on workstations and servers. However, development of formal policies and procedures is still in progress. We anticipate documentation readiness by the compliance date.

- 9. What are MedQuist's policies and procedures regarding the protection of client PHI from terminated employees who have had access to that information? Are these policies and procedures documented?**

The following actions are currently performed upon termination of employees who have had access to client PHI: company hardware/software is returned, terminated employees are removed from access lists, and physical access to company property is restricted.

- 10. Have all MedQuist personnel (including management) who are involved in the processing or manipulation of client PHI been provided with security awareness training?**

MedQuist is developing a formal workforce security awareness, education and training program, and we anticipate readiness by the required compliance date.

- 11. Are unique user identification codes required in order to access any MedQuist systems that process or manipulate client PHI?**

Yes, all MedQuist employees have unique user IDs, and only authorized users are allowed access to client PHI.

- 12. Are MedQuist users who access systems that process or manipulate client PHI educated regarding management of their passwords?**

MedQuist is developing a formal workforce security awareness, education and training program, and we anticipate readiness by the required compliance date.

- 13. Do MedQuist's systems used to process or manipulate client PHI automatically log out following a period of inactivity?**

MedQuist's new generation applications automatically log out after a specified period of inactivity.

- 14. Does the MedQuist employee handbook outline employee responsibilities for protecting the confidentiality of client PHI, or PHI in general?**

Yes.

- 15. Does MedQuist's facility security plan include how it will establish and secure access to hardware, workstations, and software used to process or manipulate client PHI?**

Yes, and the process will be reviewed and validated prior to the compliance date.



- 16. Does MedQuist have documented policies and guidelines regarding the use of computer workstations to process or manipulate client PHI, outlining the proper functions and the manner in which those functions are to be performed?**

Development of formal written procedures is in process. We anticipate readiness by the compliance date.

- 17. Does MedQuist have a documented and tested "emergency mode" operation plan that allows the organization to continue to operate and process client PHI in the event of fire, vandalism, natural disaster, or system failure?**

Yes, MedQuist has a documented and tested plan.

- 18. Does MedQuist employ a particular individual who is assigned responsibility for information security?**

Yes, MedQuist has designated a Corporate Director of Information Security and HIPAA Compliance.

- 19. Is staff access to MedQuist hardware/software that is used to process or manipulate client PHI controlled by company policies and procedures?**

Development of formal written procedures is in process. We anticipate readiness by the compliance date.

- 20. Does MedQuist have physical safeguards in place designed to eliminate or minimize the unauthorized access to client PHI through workstations?**

Yes.

- 21. What protective features does MedQuist use to verify remote access to systems used to process or manipulate client PHI?**

MedQuist employs a user ID and password system to identify remote users.

- 22. Does MedQuist encrypt client PHI that is transmitted over open communications networks (e.g., the Internet and dial-in lines) to ensure that it cannot be easily intercepted and interpreted by parties other than the intended recipient?**

Yes.

