



Center for Medicaid and State Operations/Survey and Certification Group

Ref: S&C-06-22

DATE: July 14, 2006

FROM: Director
Survey and Certification Group

SUBJECT: Privacy and Security of Beneficiary Information

TO: Survey and Certification Regional Office Management (G-5)
State Survey Agency Directors
All Contractors that Support Survey & Certification Functions

Letter Summary

Reminds survey and certification staff, State Survey Agencies, and Contractors that support survey and certification functions of the importance of protecting the privacy and confidentiality of personally identifiable health information.

Reminder to report to CMS management any breaches in ensuring privacy and security of beneficiary information.

The Centers for Medicare & Medicaid Services (CMS) wants to remind all Federal Survey & Certification Staff, State Survey Agencies, and Contractors who support Medicare survey and certification activities, of their obligation to abide by all Federal and State laws regarding confidentiality and disclosure of medical records, and other personally identifiable health information.

We further remind organizations of the necessity of effectively securing all beneficiary personally identifiable information, whether in paper or electronic format, in all locations, including the office, at home, in lodging quarters, at the provider site, and also when being transported. This includes ensuring that personally identifiable health information or data files are not saved on public or private computers when accessing corporate e-mail through the Internet and ensuring electronic systems are properly programmed for beneficiary mailings. Organizations should annually train staff on responsibilities to safeguard beneficiary information and the consequences of failing to secure sensitive beneficiary information. All organizations should either perform an internal risk assessment or engage an industry-recognized security expert to conduct an external risk assessment of the organization to identify and address security vulnerabilities. Weaknesses or gaps in your security program should be quickly remedied.

CMS considers security breaches involving beneficiary personally identifiable information to be an indication of an organization's significant non-compliance with the privacy and confidentiality

provisions in the 1864 Agreement or contracts. Failure to adhere to CMS contract terms or Agreement could lead to contract termination and/or imposition of penalties, sanctions, or remedies.

Contractors' compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy rules must be documented and kept current in response to environmental or operational changes affecting the security of the electronic protected health information. In addition, Survey & Certification staff, State Survey Agencies, and contractors should notify CMS management immediately upon discovery of any security breach compromising beneficiary personally identifiable information. For breaches involving the State Survey Agencies, the CMS Regional Office Survey & Certification management for your jurisdiction should be promptly notified. For breaches among contractors that support Survey & Certification functions, your project officer should be promptly notified.

Effective Date: This reflects current policy, guidance and instructions, but reminders to staff, State Survey Agencies, and contractors should take place no later than August 1, 2006.

Training: The information contained in this Survey & Certification Letter should be shared with all survey and certification staff, their managers, Survey & Certification Project Officers, and the state/RO training coordinators.

/s/
Thomas A. Hamilton

cc: CMS Survey & Certification Project Officers