

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop S2-26-12
Baltimore, Maryland 21244-1850



Center for Medicaid and State Operations

AUG 15 2007

Ms. Joyce Young
HIPAA GIVES Coordinator
NCDHHS-DIRM
2015 Mail Service Center
Raleigh, NC 27699-2015

Dear Ms. Young:

Thank you for your letter regarding your concern that a recent State Medicaid Director Letter (SMDL #06-022), dated September 20, 2006, may be introducing new requirements to the States in addition to those found in Federal regulations and the State Medicaid Manual.

As stated in your letter, the purpose of SMDL #06-022 was to remind State Medicaid systems and program staff of their obligation to abide by all Federal and State laws regarding the security and privacy of medical data and records, and all protected health information. Enclosed to this letter are responses addressing the questions you raised in your letter.

If you have any questions, please contact Mr. Edward C. Gendron, Director, Finance, Systems and Budget Group, at (410) 786-1064 or by e-mail at Edward.Gendron@cms.hhs.gov.

Sincerely,

Dennis G. Smith
Director

Enclosure

Page 2 - Ms. Joyce Young

Jane Alm
Privacy Officer
Oregon Department of Human Services
503-947-5255
jane.alm@state.or.us

Sheri L. Brooks
Privacy Officer
North Carolina Department of Health and
Human Services
919-855-3171
Sherri.brooks@ncmail.net

Lester Chan
Senior Consultant
California Office of HIPAA Implementation
916-654-3454
LChan@ohi.ca.gov

Frank Gose
HIPAA Privacy Officer
Kansas Health Policy Authority
785-296-4486
Frank.gose@khpa.ks.gov

Phyllis E. Hyman
Legislative and Administrative Counsel
Office of Legal Counsel, Regulations and Administrative Hearings
Connecticut Department of Social Services
860-424-5266
Phyllis.Hyman@ct.gov

Jerry Phillips
Medicaid Director
Louisiana Department of Health and
Hospitals, Office of Management & Finance
Bureau of Health Services Financing
Laurie Tichenor, contact person
225-342-9076
LTICHENO@dss.la.gov

Thea Schwartz, Esq.
AHS HIPAA Privacy Administrator
Vermont Agency of Human Services, Planning Division
802-241-4244
thea.schwartz@ahs.state.vt.us

Page 3 – Ms. Joyce Young

Lim Yong
HIPAA Project Manager
Med-QUEST Division
Hawaii Department of Human Services
808-692-8071
LYong@medicaid.dhs.state.hi.us

HIPAA GIVES Question #1:

SMDL #06-022 states that "In addition to the above HIPAA requirements, the State, in turn, should immediately report a breach, whether discovered by its own staff or reported by a contractor, to the Director of the Division of State Systems at CMS."

a. What is the legal basis for this new requirement?

CMS Response:

Under Federal regulations at 45 CFR 92.40, the State (grantee) has the following responsibilities:

- *Monitor grant and subgrant supported activities (DDI and Operations of FFP-funded Medicaid information systems) to assure compliance with Federal requirements;*
- *Submit annual performance reports to the awarding agency;*
- *Inform the Federal agency as soon as problems, delays, or adverse conditions which will materially impair the ability to meet the objective of the award become known. This disclosure must include a statement of the action taken, or contemplated, and any assistance needed to resolve the situation.*

The objective of the award is the proper and efficient operation of the jointly funded Medicaid program. Failure to properly control protected health information (PHI) represents a material impairment of a State's ability to meet this objective. Consequently, States must report to CMS privacy and security breaches with respect to any Medicaid applicant, recipient, or Medicaid system containing personally identifiable information about any applicant or recipient since not to do so will be construed as not meeting the "proper and efficient operation" condition associated with the jointly funded Medicaid program.

b. What is the definition and breadth of the term "breach" as used in the letter? For instance, does the term "breach," as used in this letter, include unsuccessful attempts to access data such as pings?

CMS Response:

A breach is any unauthorized release or disclosure of personally identifiable information about a Medicaid applicant or recipient.

The information to be protected consists of all information described in Federal regulations at 42 CFR 431.305. An authorized release or disclosure consists of provision of information covered under 431.305 that is released, disclosed or used for a purpose defined in Federal regulations at 42 CFR 431.302 as further

Although an unsuccessful attempt to obtain protected information is always cause for concern and monitoring, only breaches, as described above are required to be reported to CMS.

- c. Does this requirement to report breaches apply to both electronic and paper protected health information?

CMS Response:

Yes, it applies to both electronic and paper media.

HIPAA GIVES Question #2:

SMDL #06-022 states that "In addition, all new contracts between the State and a vendor, who is responsible for handling applicant or beneficiary data, should include a section that addresses the protection of these data and identifies specific remedies to be levied against the contractor should a negligent breach occur."

- a. What is the legal basis for the requirement to include a section that identifies specific remedies to be levied against the contractor should a negligent breach occur?

CMS Response:

CMS strongly recommends that remedies be included in all Fiscal Agent contracts to further ensure that these contractors take their role in protecting PHI seriously. Failure to include such language could result in the loss of Federal financial participation (FFP) because CMS considers holding contractors liable for the integrity of their systems' security to be a basic premise for the "proper and efficient operation" of the program.

- b. Does CMS have suggested "specific remedies"?

CMS Response:

Each State should consult with its Attorney General to determine what contract remedies are traditionally used in State contracts when contractor non-performance might be an issue.

HIPAA GIVES Question #3:

SMDL #06-022 also states that "As required by HIPAA rules, it is critical that each State include in all contracts a documented process to report breaches in privacy or security that compromise protected health information."

- a. Does this statement apply to all contracts or just Business Associate Agreements? i.e., should State Medicaid agencies require all contractors, even those that do not perform a business associate function and are not business associates, to notify the State of a breach?

CMS Response:

The Business Associate Contracts and Other Arrangements standard found in Federal regulations at 45 CFR § 164.308(b)(1) permits a business associate to create, receive, maintain, or transmit, electronic protected health information (EPHI) on behalf of the covered entity, only if the business associate receives satisfactory assurances, through a contract or other written assurance. The standard, in Federal regulations at 45 CFR § 164.314(a)(1), provides the specific criteria required for written contracts or other arrangements between a covered entity and its business associates. The actual language used to address the requirements can be tailored to the needs of each organization, as long as the requirements are addressed.

*In general, a business associate is a person or entity other than a member of the covered entity's workforce that performs functions or activities on the covered entity's behalf, or provides specified services to the covered entity, that involve the use or disclosure of protected health information. If the State has vendors who will have access to EHPI and, in the State's opinion, do not have to enter into a business associate agreement with the State, then the contracts for these vendors SHOULD have a clause that requires the vendor to report breaches to the State. This is a "should" statement because there is no statutory requirement; however, **the State is the covered entity in this case** and is thereby ultimately responsible for the safeguard of the EHPI of its beneficiaries and applicants. While this is a recommendation, not a requirement, CMS strongly recommends that in such a case the State include contract language that requires the vendor to report a breach to the State.*

- b. What is the reporting process and format?

CMS Response:

As stated in the SMDL #06-022, States should report breaches to

Attention: Richard H. Friedman, Director
Centers for Medicare & Medicaid Services
Center for Medicaid and State Operations
Finance, Systems and Budget Group
Division of State Systems
Room S3-13-15
7500 Security Blvd.
Baltimore, MD 21244-1850
Phone: (410) 786-4451
Fax: (410) 786-0370
Richard.Friedman@cms.hhs.gov

A copy should be sent to your CMS Regional Office's Associate Regional Administrator for the Division of Medicaid and Children's Health who will then notify you of further instructions.

- c. What does CMS plan to do with the information gathered?

CMS Response:

The breach data is analyzed periodically to identify possible information system weaknesses or trends that would suggest that a change in a State's security policy might be required in order to satisfy CMS' requirement that the program is being operated "properly and efficiently." Were CMS to ignore either particularly egregious breaches, or a history of poor IT system security protocols by the grantee (State), we believe we would be remiss in carrying out our financial oversight responsibilities to the American taxpayer.

- d. Will the State's funding for the Medicaid program and information systems be impacted by the number or frequency of breaches we report?

CMS Response:

Federal funding may be affected by the magnitude, number or frequency of breaches. We reserve the right to evaluate each breach on the basis of the potential harm that could be incurred, as well as the extent to which the State (as well as its contractors) had in place reasonable measures to prevent such breaches in the first place.

(45 CFR 95.612 provides that FFP for systems may be disallowed if any acquisition approved or modified under the provisions of 95.611 fails to comply with the criteria, requirements, and other undertakings described in the approved advance planning document to the detriment of the proper and efficient operation of the affected program.)

- e. The letter uses the word "should", not "must." What is the compliance expectation of "should" vs. "must"?

CMS Response:

There is no "compliance expectation" associated with the use of the term "should" in the context of direct compliance with Federal regulation. The "should statements" found in the State Medicaid Director Letter of September 20, 2006, provide guidance to the States that CMS strongly recommends the States heed. Acting on these "should statements" will help CMS and the States to properly safeguard beneficiary and applicant PHI.

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop S2-26-12
Baltimore, Maryland 21244-1850



Center for Medicaid and State Operations

SMDL #06-022

September 20, 2006

Dear State Medicaid Director:

The Centers for Medicare & Medicaid Services (CMS), Center for Medicaid and State Operations, wants to remind State Medicaid systems and program staff of their obligation to abide by all Federal and State laws regarding the security and privacy of medical data and records, and of all protected health information.

The Code of Federal Regulations (at 45 CFR 95.621) provides that State agencies are responsible for the security of all automated data processing systems involved in the administration of Department of Health and Human Services' programs, and includes the establishment of a security plan that outlines how software and data security will be maintained. This section further requires that State agencies conduct a review and evaluation of physical and data security operating procedures and personnel practices on a biennial basis.

Additionally, State agencies are required by part 11 of the State Medicaid Manual to be in compliance with the security and privacy standards contained in Pub. L. 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and adopted in 45 CFR Part 164, Subparts C and E, as follows: The security standards require that measures be taken to secure protected health information that is transmitted or stored in electronic format. The privacy standards apply to protected health information that may be in electronic, oral, and paper form.

Further, State agencies are bound by the requirements in section 1902(a)(7) of the Social Security Act (the Act), as further interpreted in Federal regulations at 42 CFR 431.300 to 307. These provisions require that use or disclosure of information concerning applicants and recipients is permitted only when directly connected to administration of the State plan.

All organizations should perform either an internal risk assessment, or engage an industry recognized security expert, to conduct an external risk assessment of the organization in order to identify and address security vulnerabilities. Weaknesses or gaps in your security program should be quickly remedied. Organizations should train staff on their responsibilities, and on the consequences of failing to secure sensitive beneficiary information, as often as is required by the security requirements outlined in this letter.

The CMS considers breaches of beneficiary security and privacy to be very serious matters. Therefore, State agencies which are found to be out of compliance with the privacy or security requirements outlined in this memorandum can expect suspension or denial of Federal financial

participation for their information systems, and may be subject to other penalties under Federal and State laws and regulations.

Under the HIPAA standards, States must also require, through business associate agreements, that fiscal agent contractors and other entities that perform claims processing, third party, or other payment or reimbursement services on their behalf protect the privacy and security of protected health information. In so doing, States should ensure that their business associates update their procedures as necessitated by environmental or operational changes affecting security and privacy. In addition, these entities must also be compliant with the requirements of section 1902 (a)(7) of the Act.

As required by HIPAA rules, it is critical that each State include in all contracts a documented process to report breaches in privacy or security that compromise protected health information. The notification of a breach should immediately be reported by the contractor to State staff following the event. In addition to the above HIPAA requirements, the State, in turn, should immediately report a breach, whether discovered by its own staff or reported by a contractor, to the Director of the Division of State Systems at CMS.

In addition, all new contracts between the State and a vendor, who is responsible for handling applicant or beneficiary data, should include a section that addresses the protection of these data and identifies specific remedies to be levied against the contractor should a negligent breach occur. It is further recommended that the State examine current contract vehicles for sections addressing the safeguarding of applicant and beneficiary data, and consider amending the contracts if provisions for specific remedies do not currently exist.

Security and privacy breaches should be reported to:

Attention: Richard H. Friedman, Director
Centers for Medicare & Medicaid Systems
Center for Medicaid and State Operations
Finance, Systems and Budget Group
Division of State Systems
Room S3-13-15
7500 Security Blvd.
Baltimore, MD 21244-1850
Phone: (410) 786-4451
Fax: (410) 786-0370
E-mail: Richard.Friedman@cms.hhs.gov

Page 3 – State Medicaid Director

I appreciate your commitment to protecting the security and privacy of our beneficiaries' health care data and personally identifiable health information.

Sincerely,

/s/

Dennis G. Smith
Director

cc:

CMS Regional Administrators

CMS Associate Regional Administrators
for Medicaid and State Operations

Martha Roherty
Director, Health Policy Unit
American Public Human Services Association

Joy Wilson
Director, Health Committee
National Conference of State Legislatures

Matt Salo
Director of Health Legislation
National Governors Association

Jacalyn Bryan Carden
Director of Policy and Programs
Association of State and Territorial Health Officials

Christie Raniszewski Herrera
Director, Health and Human Services Task Force
American Legislative Exchange Council

Lynne Flynn
Director for Health Policy
Council of State Governments