

MEMORANDUM

TO: COUNTY JUDGES, AUDITORS AND TREASURERS

FROM: REX HALL, ASSOCIATE GENERAL COUNSEL
QUINCY QUINLAN, ASSOCIATE GENERAL COUNSEL

RE: REMINDER OF HIPAA SECURITY DEADLINE

DATE: MARCH 22, 2005

As we advised all counties in our memorandum of March 25, 2003, federal law requires most counties that are subject to Health Insurance Portability and Accountability Act of 1996 ("HIPAA") be in compliance with the HIPAA Security Rule by April 20, 2005. Counties that operate a small health care plan (defined as having less than \$5,000,000 in annual premiums) have until April 20, 2006 to comply.

The HIPAA Security Rule (the "Rule") generally requires that covered entities adopt and implement policies and procedures to insure the confidentiality, integrity and availability of electronic protected health information ("EPHI"). EPHI includes any individually identifiable health information that is created, received, maintained or transmitted in an electronic format. The Security Rule requires that these policies and procedures be specifically tailored to the county's operations and resources. While there are "form policies" available, the Texas Association of Counties does not recommend using them; the county's policies must be well-suited to its particular equipment, activities and scope of operation in order to comply with the Rule.

The Scope of HIPAA

Not all Texas counties are subject to HIPAA. A more complete discussion of how to analyze whether your county is a covered entity that is subject to HIPAA can be found on the TAC website at <http://www.county.org>. At the top of the main page, there is a button called "Online Resources." Click on that button and a drop-down menu will appear. The HIPAA materials are the last item on the menu. The discussion of what entities are subject to HIPAA is contained in the general memorandum included with the HIPAA materials.

In summary, the HIPAA regulations apply to three types of entities: health plans, health care providers and health care clearinghouses. Counties typically do not operate as health care clearinghouses.

HIPAA broadly defines "health care provider" to include any person or entity that provides, or bills for the provision of, health care, including mental health care. A county likely would be subject to HIPAA as a health care provider if it provides health care services to individuals directly, such as through a county hospital or clinic.

A health plan is defined to include any “individual or group plan...that provides or pays for the cost of medical care.” A county likely would be subject to the rule as a health plan if it provides health care to its employees through a self-insured health plan, even if the county uses a third-party administrator. However, we have seen no indication that a county that participates in a self-insurance pool or purchases health insurance for its employees would be covered as a health plan.

There has been uncertainty about whether an indigent care program under Chapter 61 of the Health & Safety Code properly could be deemed a health care plan in light of the fact that the county has established a program for paying for health care provided to its indigent residents. In the context of the Privacy Rule, the Texas Association of Counties asked the Department of Health and Human Services, which is the federal agency in charge of compliance with the HIPAA Privacy Rule, to address the issue.

The Department did not provide a definitive answer, stating “[w]e are unable to render advisory opinions on the specific facts and circumstances identified in the scenarios provided by your letter or on the application of the Texas law in question.” However, after discussing the applicable law, the Department observed that, if a county “meets its indigent care obligation by establishing a program that pays the claims for health care provided, we do not see why the program would not constitute a health plan...” In light of this statement, the Texas Association of Counties believes that it would be safer for those counties with an indigent care program to consider themselves subject to both the Privacy Rule and the Security Rule. This memorandum addresses only the Security Rule. You can find additional materials pertaining to the Privacy Rule in the Online Resources section of the TAC website.

The Requirements of the Security Rule

If your county is required to comply with the Rule, it is important to read it in its entirety. The Rule can be found in the Code of Federal Regulations, at 45 CFR §164.300 and the sections that follow. You can also view the Rule at: <http://www.hhs.gov/ocr/combinedregtext.pdf>. The Rule establishes general rules for security standards, and requires each covered entity to develop and implement administrative safeguards, physical safeguards and technological safeguards designed to protect its EPHI. A summary of the Rule is set forth below

A. Security Standards: General Rules

- A covered entity must:
 1. Ensure confidentiality, integrity and availability of all electronic protected health information (EPHI) the covered entity creates, receives, maintains or transmits. Confidentiality means the property (state of being) that data or information is not made available or disclosed to unauthorized persons or processes. Integrity means property that data or information have not been altered or destroyed in an unauthorized manner. Availability means property that data or information is accessible and useable upon demand by an authorized person;

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
 3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under Privacy Rule; and
 4. Ensure that entire workforce complies with Security Rule.
- Covered entity can use any security measures that allow reasonable and appropriate implementation of the Security Rule.
 - In deciding what security measures to use, a covered entity must consider the following factors:
 1. size, complexity, and capabilities of covered entity;
 2. covered entity's technical infrastructure, hardware and software security capabilities;
 3. costs of security measures;
 4. probability and criticality of potential risks to EPHI.
 - Covered entity must comply with general security standards (which are listed above), administrative safeguards standards, physical safeguards standards, technical safeguards standards, organizational requirements standards, policies and procedures and documentation requirements standards.
 - Implementation specifications are "required" (R) or "addressable" (A). Standards involving required specifications must be implemented. For addressable specifications, the covered entity must:
 - (a) assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, in context of the specification's likely contribution to protecting the entity's EPHI;
 - (b) implement the implementation specification if reasonable and appropriate; and
 - (c) if implementing the implementation specification is not reasonable and appropriate:
 - (i) document why it would not be reasonable or appropriate to implement the implementation specification;
 - (ii) implement an equivalent alternative measure if reasonable and appropriate.
 - Security measures must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of EPHI.
- B. Administrative safeguards
- Implement policies and procedures to prevent, detect, contain, and correct security violations.

1. conduct accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI held by covered entity (R);
 2. implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the general requirements (R);
 3. sanction workforce members who fail to comply with security policies and procedures (R); and
 4. perform regular review of records of information system activity such as audit logs, access reports, and security incident tracking reports (R).
- Identify security official responsible for development and implementation of security policies and procedures.
 - Implement policies and procedures to ensure that authorized members of workforce have appropriate access to EPHI, and to prevent access to EPHI to those workforce members who do not have authorization.
 1. Implement procedures for authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed (A);
 2. Implement procedures to determine that a workforce member's access to EPHI is appropriate (A); and
 3. Implement procedures for terminating access to EPHI when workforce member's employment ends (A).
 - Implement policies and procedures for authorizing access to EPHI that are consistent with Privacy Rule.
 1. Implement policies and procedures for granting access to EPHI, e.g., through access to a workstation, transaction, program, process or other mechanism (A); and
 2. Implement policies and procedures that, based on the entity's access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program, or process (A).
 - Implement a security awareness and training program for all members of the workforce (including management):
 1. Implement periodic security updates (A); and
 2. Implement procedures for guarding against, detecting, and reporting malicious software (A);

3. Implement procedures for monitoring log-in attempts and reporting discrepancies (A); and
 4. Implement procedures for creating, changing, and safeguarding passwords.
- Implement policies and procedures to address security incidents.
 1. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes (R).
 - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (e.g. fire, vandalism, system failure, and natural disaster) that damages systems containing EPHI:
 1. Establish (and implement as needed) procedures to create and maintain retrievable exact copies of EPHI. (R);
 2. Establish (and implement as needed) procedures to restore any loss of data (R);
 3. Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of security of EPHI while operating in emergency mode (R);
 4. Implement procedures for periodic testing and revision of contingency plans (A); and
 5. Assess the relative criticality of specific applications and data in support of other contingency plan components (A).
 - Perform periodic technical and non-technical evaluation, based initially on Security Rule Standards, and subsequently in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which an entity's security policies meet the Security Rule.
 - Covered entity may permit business associate to create, receive, maintain or transmit EPHI on the covered entity's behalf only if covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information. Does not apply to:
 1. covered entity's transmission of EPHI to health care provider concerning treatment;
 2. transmission of EPHI by group health plan, HMO or health insurance issuer on behalf of group health plan to plan sponsor, to extent group health plan rules apply and are met.
 3. transmission of EPHI from or to agencies determining eligibility for government benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met (Privacy Rule requirements for agencies determining eligibility for government benefits).

- A covered entity that is the business associate of another covered entity will be in non-compliance if it violates the business associate agreement Security Rule provisions.

1. Enter into a business associate agreement with all entities the covered entity will share EPHI with.

C. Physical Safeguards

- Implement policies and procedures to limit physical access to EPHI systems and facilities in which they are housed, while ensuring properly authorized access.
 1. Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in event of an emergency (A);
 2. Implement policies and procedures to safeguard facility and equipment from unauthorized physical access, tampering, and theft (A);
 3. Implement procedures to control and validate a person's access to facilities based on their role and function, including visitor control, and control of access to software programs for testing and revision (A);
 4. Implement policies and procedures to document repairs and modifications to physical components of a facility that are related to security (e.g. hardware, walls, locks, doors) (A); and
 5. Implement policies and procedures specifying the proper functions, manner of performing those functions, and physical attributes of surroundings, of a specific workstation or class of workstations that can access EPHI (A).
- Implement physical safeguards for all workstations that access EPHI so that only authorized users have access.
- Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and within the facility.
 1. Implement policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored (R);
 2. Implement procedures for removal of EPHI from electronic media before media are made available for re-use (R);
 3. Maintain record of movements of hardware and electronic media and any person responsible therefore (A); and
 4. Create retrievable, exact copy of EPHI, when needed, before moving equipment (A).

D. Technical Safeguards

- Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights.
 1. Assign unique name and/or number for identifying and tracking user identity (R);
 2. Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency (R);
 3. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity (A); and
 4. Implement a mechanism to encrypt and decrypt EPHI (A).
- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.
- Implement policies and procedures to protect EPHI from improper alteration or destruction.
 1. Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner (A).
- Implement procedures to verify the identity of a person or entity seeking access to EPHI.
- Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.
 1. Implement security measures to ensure EPHI is not improperly modified without detection until disposed of (A).
 2. Implement a mechanism to encrypt EPHI whenever deemed appropriate (A).

E. Organizational Requirements

- Contracts with business associates (those with whom you might share EPHI in performing your operations) must require business associate to:
 1. implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI the BA creates, receives, maintains, or transmits on behalf of the covered entity (R);
 2. ensure that agents, including subcontractors, to whom it provides EPHI, agree to implement reasonable and appropriate safeguards to protect EPHI (R);
 3. report to covered entity any security incident of which it becomes aware (R); and

4. authorize covered entity to terminate the contract, if covered entity determines BA has violated a material term of the contract (R).
- A covered entity violates the Security Rule if it knew of a Business Associate's pattern of activity or practice that constituted a material breach or violation of the Business Associate contract, unless the covered entity took reasonable steps to cure the breach, and if such steps were unsuccessful:
 - (a) terminated the contract; or
 - (b) if termination were infeasible, reported the problem to HHS.
 - A group health plan's plan documents must provide that plan sponsor will reasonably and appropriately safeguard EPHI created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan. There is an exception for EPHI disclosed to a plan sponsor under 164.504(f)(1)(ii) (plan document amendment requirements under Privacy Rule), or 164.508 (authorization requirements under Privacy Rule).
 - Plan documents must be amended to require plan sponsor to:
 1. implement administrative, physical, and technical safeguards that reasonably and appropriately protect EPHI the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits on behalf on behalf of the group health plan (R);
 2. ensure that the adequate separation between plan sponsor and plan required by the Privacy Rule is supported by reasonable and appropriate security measures (R);
 3. ensure that any agent, including subcontractor, to whom it provides EPHI, agrees to implement reasonable and appropriate security measures to protect the EPHI (R); and
 4. report to group health plan any security incident of which it becomes aware (R).

F. Policies and procedures and documentation requirements

- A covered entity must:
 1. Implement reasonable policies and procedures to comply with Security Rule. Covered entity may change its policies and procedures at any time, if the changes are documented, and implemented in accordance with the Security Rule;
 2. Maintain in written form (electronic OK) the policies and procedures that were implemented;
 3. If an action, activity or assessment must be documented, maintain a written version (electronic OK);
 4. Retain documentation for 6 years from date of creation, or date when it was last in effect, whichever is later; and

5. Make documentation available to the persons responsible for implementing the procedures to which the documentation pertains.
- Review documentation periodically and update as needed.

Conclusion

Compliance with the Rule cannot be achieved overnight; it requires a process of learning your operations and equipment, identifying risks and addressing them, and training your employees in the procedures that ultimately are developed. Compliance will require a cooperative effort among a number of individuals, and it will require these individuals to understand the county's computer systems and how electronic data are managed. Any management-level individuals involved in the covered operations (whether these operations are as a health plan or a health care provider) must be included in the process, as should any elected official or employee with expertise in information systems. In addition, your county's effort to comply would be well-served if you can obtain assistance from an attorney, as well as someone with a computer security background.

We hope this information has been helpful to you. The Legal Department of the Texas Association of Counties is distributing this memorandum as a public service. This memorandum is not legal advice. It does not take the place of discussions with your county attorney or other legal counsel, HIPAA consultants or other computer security consultants.