



UPDATE

PRACTICE MANAGEMENT

Volume 25, Number 3

September 2007

Questions HHS Might Ask During a HIPAA Security Audit

Compliance with the HIPAA Security Rule became effective on April 20, 2005. At that time, many practices went through the motions of reviewing checklists that outlined the necessary and addressable processes required by the Rule. In the two years since the Rule's implementation, many situations have changed in many medical practices. The implementation of new practice management systems and electronic medical records has not only changed the manner in which data is processed, but also likely changed your practice's electronic and other security needs as they are covered under the Security Rule.

While it may not seem relevant to your practice, it is of note that in March 2007 one of Atlanta's Hospitals became the first institution in the country to be audited for compliance with the HIPAA Security Rule.

The audit was conducted by the Office of the Inspector General of the U.S. Department of Health and Human Service (HHS). Many in the health care industry view this as a precursor of similar audits to come at other institutions, and possibly large medical practices.

Since March there has been little public discussion regarding the actual occurrence of the audit and its outcome. However, information has leaked on the nature of the questions asked and information sought by the OIG. Do you have current policies and procedures in place that describe the following?

1. Method for establishing and terminating users' access to systems housing electronic patient health information (ePHI).
2. How you gain emergency access to electronic information systems?
3. What occurs during inactive computer sessions (periods of inactivity)?
4. Recording and examining activity in information systems that contain or use ePHI.
5. Risk assessments and analyses of relevant information systems that house or process ePHI data.
6. How you address employee Security Rule violations (sanctions)?
7. Electronically transmitting ePHI.
8. Preventing, detecting, containing and correcting security violations (incident reports).
9. Regularly reviewing records of information system activity, such as audit logs, access reports and security incident tracking reports.
10. Creating, documenting and reviewing exception reports or logs.
11. How you routinely monitor systems and the network, including a listing of all network perimeter devices, i.e., firewalls and routers?
12. Physical access to electronic information systems and the facility in which they are housed.
13. Establishing security access controls; (what types of security access controls are currently implemented or installed in hospitals' databases that house ePHI data?).
14. Remote access activity i.e. network infrastructure, platform, access servers, authentication, and encryption software.
15. Internet usage.
16. Wireless security (transmission and usage).
17. Firewalls, routers and switches.
18. Maintenance and repairs of hardware, walls, doors, and locks in sensitive areas.
19. Terminating an electronic session and encrypting and decrypting ePHI.
20. Transmitting ePHI.
21. Password and server configurations.
22. Antivirus software.
23. Network Remote Access.
24. Computer Patch Management.

Inside This Edition

Questions HHS Might Ask During a HIPAA Security Audit.....	1
Medicaid & Tamper Proof Prescription Pads.....	2
Underutilized Opportunity in a 1031 Property Exchange.....	3
Company News.....	4

Continued on Page 2

Your Tax Dollars at Work . . . “Tamper-Proof” Prescription Pads Mandated on October 1



In the most unusually titled “U.S. Troop Readiness, Veterans’ Care, Katrina Recovery, and Iraq Accountability Appropriations Act of 2007,” Congress included Section 7002(b) which states, “Effective Oct. 1, 2007, Medicaid outpatient drugs will be reimbursable only if nonelectronic written prescriptions are executed on a tamper-resistant pad.”

The Centers for Medicare & Medicaid Services (CMS) will likely send a letter to state Medicaid directors regarding state implementation of this federal requirement. State insurance commissioners will likely have the ultimate implementation authority through a state definition of tamper-proof prescription pad. California, Florida, Idaho, Indiana, Kentucky, Louisiana, Massachusetts, Mississippi, New Jersey, New York, Pennsylvania, Texas and Wyoming already have laws

requiring varying levels of tamper-proof prescription pads. These states variously require prescription pads to be written in triplicate; require pads to contain chemicals that reveal efforts to alter the paper; or require pads to display serial numbers so pharmacists can match the physician’s orders.

It is not clear if this new federal requirement will apply to all drugs or just narcotics. Although the law’s intent is to prevent patients from obtaining drugs illegally, the rapidly approaching start date leaves little time for education and compliance for pharmacists, physicians and the 55 million Medicaid beneficiaries.

Of course, if you are submitting prescriptions electronically, this regulation is of little concern.

For additional information, visit your State Medicaid website.

Questions HHS Might Ask During a HIPAA Security Audit

Continued from Page 1

If requested by the OIG, could you easily provide the following information?

1. A list of all information systems that house ePHI data, as well as network diagrams, including all hardware and software that are used to collect, store, process or transmit ePHI.
2. A list of terminated employees.
3. A list of all new hires.
4. A list of encryption mechanisms used for ePHI.
5. A list of authentication methods used to identify users authorized to access ePHI.
6. A list of outsourced individuals and contractors with access to ePHI data, if applicable.
7. A list of transmission methods used to transmit ePHI over an electronic communications network.
8. Organizational charts that include names and titles for the management information system and information system security departments.
9. Entity wide security program plans (e.g., System Security Plan).
10. A list of all users with access to ePHI data and each user’s access rights and privileges.
11. A list of systems administrators, backup operators and users.
12. A list of antivirus servers, installed, including their versions.
13. A list of software used to manage and control access to the Internet.
14. The antivirus software used for desktop and other devices, including their versions.
15. A list of users with remote access capabilities.
16. A list of database security requirements and settings.
17. A list of all Primary Domain Controllers (PDC) and servers (including Unix, Apple, Linux and Windows) that are used for processing, maintaining, updating, and sorting ePHI.
18. A list of authentication approaches used to verify a person has been authorized for specific access privileges to information and information systems.

If the answer is “no” to any of the above, it’s time to reassess and regain control of security in your practice. Be prepared! Contact Heather Long at Gates, Moore & Company to order a comprehensive compliance guide to the HIPAA Security Rule today!

Underutilized Opportunity in a 1031 Exchange



Under **Internal Revenue Code (IRC) Section 1031**, a real property owner can sell certain property and then reinvest the proceeds in ownership of like-kind property and defer the capital gains taxes. To qualify as a like-kind exchange, property exchanges must be done in accordance with the rules set forth in the tax code and in the treasury regulations. The 1031 exchange can offer significant tax advantages to real estate buyers allowing a greater portion of the proceeds to be reinvested and to continue to be deferred. An underutilized opportunity in this type of real estate transaction is a Tenants-in-Common (TIC) ownership arrangement.

What is Tenants-in-Common?

TIC ownership is a form of real estate asset ownership in which two or more persons have an undivided, fractional interest in the asset, where ownership shares are not required to be equal, and where ownership interests can be inherited. Each co-owner receives an individual deed at closing for his or her undivided percentage interest in the entire property. Through TIC ownership, the average qualified owner of investment real estate is able to enjoy ownership in an institutional-type property with a lower or smaller investment.

The TIC structure has various features that make it attractive to the real estate buyer:

Access to Higher Grade Properties - The typical entrance in whole commercial building begins at \$1 million, but through co-ownership as a Tenants-in-Common, the potential purchaser of investment real estate is able to enjoy ownership in an institutional-type property with a lower or smaller purchase price. Besides reliable income and growth potential, TIC properties are typically able to attract tenants with greater financial strength and stability than smaller, less quality properties.

Combined Real Estate Experience - As an alternative to sole ownership of real estate, an experienced buyer of investment real estate can take ownership in a large commercial property along with other unrelated buyers, not as limited partners, but as individual TIC owners. Each of the TIC owners brings their previous real estate knowledge to the group. Thus, each decision of the TIC ownership will be backed by many years of real estate experience.

Exact Dollar Matching - In TIC properties, a qualified owner of investment real estate can purchase any percent desired in the property (subject to minimum requirements). For example, if you have \$152,479 of equity from the sale of a previous property you can purchase \$152,479 of equity in a TIC property.

Reasonable Purchase Price - Revenue Procedure 2002-22 issued by the IRS allows up to 35 TIC owners in any one property. Thus, the purchase price reflects ownership by multiple experienced buyers making the price reasonable for such quality properties with a minimum purchase price of \$150,000 for well-qualified and experienced buyers.

Diversification - Due to the low minimum purchase price in TIC properties, an experienced buyer can diversify into different properties in various different marketplaces based upon the buyer's individual needs and expertise.

Deeded Interest - The TIC owners buy the property and receive a deeded interest. You can transfer this interest by gift, sale, inheritance, assignment, etc. Such transfer does not need to coincide with the transfer of all TIC interests in the property.

No Special Allocations - All the TIC owners receive monthly rental payments, sale proceeds and the depreciation tax benefits in proportion to their percentage ownership in the property.

Disclaimer: The above brief description should not be construed as legal or tax advice.

Please contact Gates, Moore & Company if you would like assistance evaluating the pros and cons of a 1031 exchange.

Retirement Planning and Exit Strategies for Physicians

WHAT: SEMINAR AND DINNER (PHYSICIANS ONLY)

WHEN: WEDNESDAY, NOVEMBER 7TH, 2007

TIME: 5:30 P.M. TO 7:30 P.M.

WHERE: CHEROKEE COUNTRY CLUB

RSVP TO: HLONG@GATESMOORE.COM

SEATING IS LIMITED.

Company News



MRG Medical Solutions celebrates its one year anniversary in Georgia and has brought immediate results to practices all over the region.

Increased collections - A specialty physician transitioned to MRG from another billing service after experiencing erratic collections despite steady productivity and payor mix. MRG improved her collections by 39% more on average per month by identifying billing errors of the previous company and identifying the misuse of a modifier that caused unnecessary denials. MRG also helped this practice appeal and rebill previously denied claims to collect much of that money that otherwise would have been written off.

Decreased Expenses/Increased Flexibility - A primary care physician starting private practice quickly discovered that most reputable software programs are expensive and required some network administration knowledge. For a monthly fee and no upfront cost, she instead chose to utilize our ASP timeshare arrangement to access the General Electric (GE) Centricity practice management system. MRG handles the data backup, updates, training and support. The practice is required to only have PC workstations and high speed internet access. This solution works perfectly for those who don't want to spend thousands of dollars to get started but want to perform their own billing. An added benefit - MRG's billing staff can remotely fill in as needed and keep billing processes going during times of employee absence or turnover.

Billing Services now available to eClinicalWorks (ECW) users! We are pleased to announce that MRG can now provide billing and accounts receivable management services for those practices utilizing the eClinicalWorks practice management system through remote log-in technology. If you are an established ECW user, you can now outsource your billing without additional costs for software or hardware.

MRG Medical Solutions has a solution that can be customized for you.

To discuss how the services of MRG Medical Solutions may be of benefit to your practice, please contact Randy Penberg directly at 678-553-8150 or toll free at 877-553-8150 or via email at info@mrgga.com.

Congratulations Valerie!

We are excited to announce Valerie Rock has completed her apprenticeship (CPC-A) and is now fully credentialed as a Certified Professional Coder (CPC). Congratulations, Valerie!

*Update: Practice Management
is published quarterly for clients by
Gates, Moore & Company
Your questions and comments may be
directed to:*

*Gates, Moore & Company
Tower Place 100, Suite 600
3340 Peachtree Road, N.E.
Atlanta, GA 30326
Phone: (404) 266-9876*

PUTTING EFFECTIVE MANAGEMENT INTO PRACTICE

*Presort Standard
U.S. Postage Paid
Permit #6581
Atlanta, GA*

Gates, Moore & Company
3340 Peachtree Road, N.E.
Tower Place 100, Suite 600
Atlanta, GA 30326