

LEGAL ALERT

September 2003

HEALTH CARE LAW UPDATE

Health Care, HIPAA, and Information Technology

ARE YOU PREPARED FOR THE TCS DEADLINE?

Many healthcare providers have been so focused on compliance with the HIPAA Privacy Regulations that they have not paid much attention to the electronic Transactions and Code Sets (TCS) portion of the law. The deadline for compliance with TCS is October 16, 2003. To date, CMS has not been receptive to a delay in the deadline. Note the following article:

July 24, 2003 – During a Special Open Door Forum on HIPAA this afternoon, the Centers for Medicare and Medicaid Services (CMS) presented guidance on compliance with the October 16 transactions and code sets (TCS) deadline. In response to inquiries received expressing concern over the health care industry's state of readiness, the Department of Health and Human Services issued the guidance outlining its approach to enforcement of the TCS provisions. The guidance reiterates what CMS officials have been saying all along: "The law is clear: October 16, 2003 is the deadline... after that date, covered entities, including health plans, may not conduct noncompliant transactions" and "CMS will focus on obtaining voluntary compliance and use a complaint-driven approach for enforcement..."

The most significant risk for missing the deadline is not an investigation due to a complaint filed against your entity. It is the risk of an abrupt interruption of your cash flow due to non-payment by payers as a result of noncompliance with the transaction requirements. It has been estimated that the average provider cannot last financially for

more than 10-14 days with an interruption in claims payments. It is not unrealistic to believe it will take weeks, if not months, to become compliant and resubmit your claims for payment.

If you haven't already begun your TCS testing, don't panic. Immediately begin the process by developing a testing strategy and plan. Major steps to include in this process are:

- Assign responsibility for testing.
- Speak to your external partners, including those for your software applications, your payers and any clearinghouses. Discuss delivery dates for new software and the support they provide for data conversion and testing.
- Develop a broad set of test scenarios, cases, and scripts.
- Be sure that all system changes (vendors, clearinghouses, and any internal custom code requiring remediation) are scheduled and incorporated into the test plan.

Key Questions for Vendors and Clearinghouses

Do not assume your vendor or clearinghouse is HIPAA compliant. Communicating with them is the key. For a list of questions you can ask your vendors, third party administrators, and clearinghouses, go to: <http://www.cms.hhs.gov/hippa/hippa2/questionsforproviders/askvendors.pdf>

- Identify your transaction certification strategy and contact the appropriate vendors well in advance to inform them of your plan.
- Obtain specific information from your trading partners about their testing processes and procedures. Be sure to incorporate those parameters into your test plan.
- Make a realistic assessment of the resources needed to initiate the test plan.
- Incorporate the major elements of your Transaction Contingency Plan into your test plan.
- Document everything. Maintain a record of your entire testing process from planning to final sign-off.

It may be advantageous to utilize consultants to augment your internal initiatives. Based on the Phoenix Spring 2003 Healthcare Industry HIPAA Survey, 44% of respondents across the industry are currently using outside consultants to support HIPAA initiatives. As in the past, the biggest users of consultants are larger hospitals (46% of which use consultants) and Payers (66%). Approximately 30% of respondents have engaged consultants for assessment and implementation planning services, 22% for implementation support, and about 45% for HIPAA awareness and training support.

The Phoenix Survey asked providers and payers to indicate which types of Transactions their organizations were actually planning to send and receive, at least as of the October 16 deadline. Not surprisingly, payer projections are greater than those of providers, considering the requirements upon them to handle all HIPAA standardized Transactions. The majority of Providers anticipate conducting 837 Claims and 835 Payments and Remittance Advice Transactions immediately. However, a majority of Providers do not plan to conduct the remaining standard electronic Transactions, at least as of October 2003.

Transaction Types	Providers	Payers
837 Claims, COB, Equivalent Encounter	76%	84%
835 Payment, Remittance Advice	55%	80%
270/271 Claims Status	32%	71%
276/277 Eligibility	29%	66%
834 Enrollment/Disenrollment	13%	56%
820 Premium Payment	6%	45%
None	1%	3%

Is it too late to get started? Technically, yes. You should have already begun testing, as required under ASCA. For many covered entities, the reality is they must **get started now** if they have not begun the testing process. Do not wait for your vendor or clearinghouse to determine your testing approach. Remember, you are the covered entity responsible for compliance and it was you who signed and certified the ASCA Compliance Extension Form back in October. It is your organization that must achieve TCS compliance in only a few weeks...and most important, it is your organization that will lose revenues if your submitted claims cannot be paid!

This article was submitted by the principals of the HIPAA Compliance Advisors, John Cromer and John Kandra. For more information, you can contact them at (616) 364-7570 or at hcam@comcast.net.

Electronic Submission of Medicare Claims

The Center for Medicare & Medicaid Services (CMS) has issued an interim final rule with comment period on the electronic submission of Medicare claims. Published in the Federal Register on August 15, 2003, the regulations implement the HIPAA-mandated requirement that claims for reimbursement under Medicare be submitted electronically as of October 16, 2003. Absent an applicable exception or waiver (spelled out in the rule), paper claims submitted to Medicare after October 16, 2003, will NOT be paid.

NEW SECURITY REGULATIONS: THE NEXT STEP UNDER HIPAA

On February 20, 2003, the Department of Health and Human Services (DHHS) published the final rule adopting standards for the security of electronic protected health information. The final rule implements some of the requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Like the HIPAA privacy rule, the security regulations apply to all “covered entities”: health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a covered transaction.

The Purpose behind the Security Rule

The purpose of the final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Electronic protected health information is individually identifiable health information that is transmitted by or maintained in electronic media. Electronic media includes memory devices, removable digital memory medium, such as magnetic tapes or disks, the Internet, intranet, leased lines, dial-up lines, and private networks. It does not include the transmission of paper via facsimile or of voice via telephone.

Under the rule, covered entities should: (1) protect against reasonably anticipated threats or hazards to the security and integrity of electronic protected health information; (2) protect against reasonably anticipated uses and disclosures of electronic protected health information not permitted under the rule; and (3) ensure compliance by its workforce.

According to DHHS, the security standards are based on three general concepts. First, the standards were developed to be flexible and scalable, allowing covered entities to interpret and implement the standards in accordance with their own risks. Second, the standards are comprehensive, covering all aspects of security, behavioral as well as technical. Third, the standards are technology neutral, allowing covered entities to use future technological advances

without requiring DHHS to modify the standards.

Security vs. Privacy

The security rule differs in scope from the privacy rule in two important ways. While the privacy rule covers all protected health information, whether in paper, electronic or oral format, the security rule only applies to electronic protected health information. In addition, while the privacy rule covers only the confidentiality of information, the security rule contains standards that address both the integrity and availability of electronic information. Under the security rule, covered entities are required to enact policies and procedures that ensure that electronic data is not inappropriately changed and that it is available when needed.

The Substance of the Rule

The security rule adopts both standards (general requirements) and implementation specifications (specific measures that pertain to a particular standard). There are 18 administrative, physical, and technical standards. Examples of these standards include security management process, security awareness and training, workstation use, access control, and person or entity authentication, among others. There are 36 implementation specifications associated with these standards, only 14 of which are mandatory and 22 of which are “addressable.” There are also 6 additional standards which cover organizational requirements, policies and procedures, and documentation.

If an implementation specification is “addressable,” a covered entity should assess whether the implementation specification is a reasonable and appropriate safeguard in its environment. If it is, the covered entity should implement it. If it is not, the covered entity should document why it is not reasonable and appropriate, and implement an equivalent alternative measure. This concept of “addressability” transfers the judgment making process from DHHS to the covered entity, allowing the covered entity to make its own decisions regarding risks and the most effective

mechanisms to reduce those risks. All of the security standards and implementation specifications are summarized in a matrix “cheat sheet,” which was published as part of the final rule.

Getting Started

Covered entities should begin their compliance efforts with a risk analysis of their systems. Based upon this assessment, each covered entity should determine how best to implement each standard and implementation specification (even addressable ones). Documentation of the risk assessment, the determination of how to implement each standard, and all policies and procedures are essential. Each covered entity should then train its workforce and conduct

periodic evaluation of its systems and policies and procedures.

Covered entities, excluding small health plans that will have an extra year to comply, should be in compliance with the new security standards by April 21, 2005. While the deadline for compliance may seem far away, we recommend that all covered entities begin the risk assessment process as soon as possible.

This article was written by Ashley W. Taylor. For more information on the security regulations, please contact any member of the HIPPA compliance team: Christopher R. Genter, R. Jay Hardin, Richard C. Kraus, Veronica A. Marsich, Rachel Brochert Roe, or Ashley W. Taylor.

ADVANCES IN INFORMATION TECHNOLOGY IN THE HEALTH CARE INDUSTRY

The health care industry is undoubtedly one of the most data-intensive industries in the U.S., yet it has traditionally been behind the eight ball when it comes to information technology—falling far behind other industries such as banking, insurance and retail. While most health care innovations have recently focused on diagnoses and treatment, many providers are realizing that information technology will play an increasingly important role in the field of medicine, especially with respect to patient safety. Despite growing evidence that electronic medical records can reduce medical errors and improve patient care, fewer than 5% of America’s primary-care providers and only 10% to 20% of hospitals use such systems, according to a recent *Wall Street Journal* article.

Benefits of Electronic Medical Records and Information Technology

One of the many benefits of electronic medical records and information technology in health care is the obvious beneficial effect on physician behavior and care processes. Electronic medical records allow providers to access information from a variety of locations and to render care appropriately. Multiple users may also access the records simultaneously. Such availability is

especially important in multi-site institutions, where it may be impossible to move a physical file around. Health care providers will also save money on paper storage, filing costs, and time spent searching for physical records. Institutions will be able to analyze records more thoroughly, detect errors more quickly, determine reimbursement rates, and justify reimbursement claims.

In addition, the benefits of electronic medical records extend beyond the institutions that use them. Electronic records also allow health care providers to share information more readily with other providers at different sites, reducing the number of redundant queries and diagnostic tests and improving the availability of health-related information at the point of care delivery. On a global scale, the ability to quickly gather and share medical information for public health purposes has become increasingly important, especially in light of terrorism and recent epidemics like SARS and the West Nile virus.

Obstacles to Electronic Medical Records and Information Technology

Despite the many benefits of electronic medical records and information technology, the road to

adoption of such innovations is long and full of obstacles. Certainly, the capital investment required to implement an electronic medical record system at any one institution may be prohibitive. In addition, it is also difficult to capture data from health care professionals in a structured and computer-friendly manner. Physicians who are accustomed to dictating free-text health information may find the transition to an electronic system challenging.

In addition, most existing electronic data sources in the health care industry operate independently of each other, with different structures and different coding systems. Not only might a laboratory have a different system than an outside physician's office or pharmacy, but it also may differ from other departments within the same hospital. The key to information technology success in the health care industry is to make all of these different systems learn to communicate with each other. Such communication may be facilitated, in part, by the creation, adoption, and support of industry standards.

Industry and Federal Action

The health care industry appears to have realized the benefits it can gain from investing money in information technology. Spending on healthcare information technology by providers is likely to increase from \$ 15.1 billion in 2002 to \$17.3 billion in 2007, according to new research from the International Data Group. Increasingly, this money will be spent on clinical, rather than administrative, functions, such as computerized physician order entry.

The Bush administration has also vowed to seek a 53% increase in funding to help hospitals use information technology to keep better records. As part of the administration's new focus on information technology, on July 1, 2003, the U.S. Department of Health and Human Services (HHS) Secretary Tommy Thompson announced two steps in building a national electronic health care system that will allow patients and their doctors to access their complete medical records anytime and anywhere they need.

First, the Secretary announced that HHS has signed an agreement with the College of American Pathologists (CAP) to license the College's

standardized medical vocabulary system known as SNOWMED (Systematized Nomenclature of Medicine) Clinical Terms and make it available without charge throughout the U.S. This action opens the door to establishing a common medical language as a key element in building a unified electronic medical records system in the U.S.

With terms for more than 340,000 medical concepts, the College's standardized system has been recognized as the world's most comprehensive clinical terminology database available. The licensing agreement with the CAP will make it possible for health care providers, hospitals, insurance companies, public health departments, medical research facilities, and others to easily incorporate this uniform technology into their information systems.

Secondly, the Secretary announced that HHS has commissioned the Institute of Medicine to design a standardized model of an electronic health record. Health Level Seven, Inc. (HL7), a health care standards development organization in Ann Arbor, Michigan, has been asked to evaluate the model once it has been designed. HHS expects to have a standardized record ready in 2004.

Earlier this year, the Department of Health and Human Services, Defense, and Veteran Affairs also announced the first set of uniform standards for the electronic exchange of clinical health information to be adopted across the federal government. The three federal departments that deliver health care services are coordinating with numerous other federal agencies to standardize federal clinical health information. The new standards will help improve the quality of care by ensuring that federal entities use a common coding system that will make it easier to coordinate care and exchange needed information.

"It's important for the federal government to lead by example by selecting and adopting these standards," said HHS Secretary Thompson. "With appropriate privacy protections for personal health information, consumers and patients will benefit when their health information is available to their doctors and other health care providers when it is needed, such as in the emergency rooms. But we cannot do it alone

The private sector will be crucial to the widespread diffusion of these standards.”

The Federal government has also helped jump start the adoption of national standards with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA not only requires health care providers, clearinghouses, and health plans to transmit information in standard formats in connection with certain electronic transactions, but it also requires these entities to implement various security measures to protect the confidentiality and integrity of the electronic health information they store and transmit.

If you are thinking about moving to electronic medical records, be sure to consider all of the benefits and obstacles, as well as current industry and federal issues, in deciding whether such a transition is appropriate for your organization.

This article was submitted by the Health Care Law Department at Smith Haughey Rice & Roegge.

The Members of
SMITH HAUGHEY RICE & ROEGGE'S
Health Care Law Department are:

William W. Jack, Chair	(616) 458-6243	Grand Rapids
William R. Jewell	(616) 458-8203	Grand Rapids
Christopher R. Genter	(616) 458-0222	Grand Rapids
R. Jay Hardin	(231) 486-4534	Traverse City
Richard C. Kraus	(517) 318-5653	Lansing
Veronica A. Marsich	(517) 332-3030	Lansing/Ann Arbor
Rachel Brochert Roe	(231) 486-9503	Traverse City
Ashley W. Taylor	(734) 913-6907	Ann Arbor