BNA, INC.

ELECTRONIC COMMERCE & LAW

BNA Employee-Owned Since 1947

VOL. 8, NO. 22 PAGES 541–572 REPORT JUNE 4, 2003

HIGHLIGHTS

Search Engine Result Rankings Are Opinions Protected by Constitution
Web site rankings that form the results of a search engine operation are opinions that constitute protected speech under the First Amendment of the U.S. Constitution, a federal district court in Oklahoma rules. The court further holds that under Oklahoma law constitutionally protected speech such as search engine rankings are per se lawful and thus may not give rise to an action for tortious interference with business relations. **Page 557**

Lanham Act No Bar to Unaccredited Copying of Public Domain Work
The Lanham Act does not prevent the unaccredited copying of a work whose copyright has expired, the U.S. Supreme Court holds unanimously. The producer of the copies is the ''origin'' of those goods and thus does not falsely designate their origin or otherwise engage in misrepresentation prohibited by the statute when it sells the copies as its own products without attribution to the creator of the original, Justice Scalia says. **Page 550**

Ban on Publication of Police Personal Data Violates First Amendment
A state law that prohibits the publishing of information about police personnel is facially unconstitutional under the First Amendment, a federal district court in Washington rules. **Page 551**

Seizure of Data in Violation of Contract Subject to Claim Under CFAA
The forcible entry into the computer room and the unauthorized copying of data constituted a violation of the Computer Fraud and Abuse Act of 1986, a federal district court in Florida rules. The court also holds that expenses incurred in order to investigate and respond to various attempts to access data qualifies as loss under the CFAA. **Page 553**

Even Small Choices in Software Design Subject to Infringement Action
Formatting choices in a computerized form may constitute copyrightable expression subject to an infringement claim, regardless of the small degree of ''originality'' involved, the Seventh Circuit rules. When it comes to a copyright infringement claim, the degree of originality of a work is relevant only to the extent that it is copyrightable, the court says. **Page 554**

Lead Report

CONTENT REGULATION: The California Supreme Court hears oral arguments in a case involving the constitutionality of a trial court's preliminary injunction—based on trade secret law—barring a Web site operator from publishing on the Internet a computer program that defeats a proprietary encryption scheme protecting motion pictures recorded on digital video discs. First Amendment issues are at the forefront, but other important legal questions are in the mix, such as whether widespread Internet posting destroys a trade secret and whether a click-wrap contract may prohibit otherwise lawful reverse-engineering. **Page 545**

ALSO IN THE NEWS

CONTENT REGULATION: An Internet forum is not liable for posters' opinions, and the operator need not monitor posts for legal violations, a German regional court rules. **Page 552**

FEDERAL PREEMPTION: The Fourth Circuit orders reconsideration of a decision regarding the constitutionality of alcohol sales restrictions after action by the legislature. **Page 556**

MARKETING PRACTICES: A French court rules that a political organization with strong ties to the French government had violated the law with a spam attack intended to slow an ongoing protest movement led by three labor unions. **Page 555**

MARKETING PRACTICES: Nine actions involving the Internet advertising company Gator Corp. are transferred to a federal district court in Georgia by the Judicial Panel on Multidistrict Litigation. **Page 555**

EXPERT REPORT

PRIVACY: Responsible groups predict that the October 2003 deadline for implementing HIPAA's privacy mandates will not be met. The author reviews the history of the regulation, relevant legal issues, the potential impact of a failure in implementation, and options for averting a HIPAA logjam. **Page 559**

 ISSN 1098-5190

Expert Report

HIPAA STANDARD TRANSACTIONS

Responsible groups predict that the October 2003 deadline for transitioning to HIPAA standard transactions will not be met, and that consequences may include a disastrous disruption in health care reimbursements and cash flow. The transition is complicated by confusion about how federal and state law affect HIPAA standard transactions. A fuller understanding of those legal principles may mitigate—though it cannot eliminate—the potential disruption that is less than five months away.

Surviving Standard Transactions: A HIPAA Roadmap

BY RICHARD D. MARKS

On Oct. 16, by law, most of the U.S. health care industry must switch to a system of standard computer transactions for medical payments and related inquiries regarding health insurance. This switch, mandated by HIPAA[1], is probably the largest conversion of computer systems in history.

HIPAA's vision is the creation of a nationwide system of electronic data interchange (or EDI) to standardize the business of enrolling patients for health insurance, verifying their eligibility for coverage, making and paying claims for health care, and performing related information exchanges efficiently, electronically, and without resort to paper.[2] To enforce this vision, the statute (and implementing rules from the U.S. Department of Health and Human Services) requires the health care industry to abandon the hodgepodge of proprietary transaction formats and codes, and move instead to new, government-prescribed ''standard transactions.''[3]

Success depends on the government's timely development of understandable standards for computer processing that will work nationwide, and the health care industry's conversion of its computer systems and associated business processes to the new mandatory standards.

With less than five months to go, there are serious doubts that the conversion will go smoothly. Some well-known groups fear there may be substantial problems, because the computer systems of large segments of the health care industry will not be ready to process the new standard transactions successfully.

For example, the Workgroup for Electronic Data Interchange (known as WEDI) is one of four entities with which the HHS secretary must, by statute, consult in administering HIPAA.[4] On April 15, WEDI's chairman wrote to the HHS secretary, stating that ''a substantial number of covered entities are not sufficiently far along to achieve compliance with HIPAA Transaction and Code Set (TCS) standards by . . . October 16, 2003.''[5] He asked the secretary to provide guidance, and framed the problem this way: ''[H]ow does the industry make the short-term transition from its current state to a suc-

[1] The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, enacted Aug. 21, 1996 (codified at 42 U.S.C. § 1320d).

[2] *See South Carolina Medical Association v. Thompson*, 327 F.3d 346, 348 (4th Cir. April 25, 2003).

Richard D. Marks is a partner in the Washington, D.C., office of Davis Wright Tremaine. He is co-chairman of the Security Policy Advisory Group of the Workgroup for Electronic Data Interchange, one of the four consultative entities named in the HIPAA statute, and is chair of the HIPAA Task Force of the ABA Section of Science and Technology Law. While this article analyzes legal issues relating to HIPAA, it is not legal advice, and is not intended, nor should it be used, as a substitute for legal advice. Marks represents certain entities mentioned by name or role in this article. However, the views expressed are his own, and not those of any client or of Davis Wright Tremaine.

[3] 42 U.S.C. § 1320d-2. The standard transactions listed in that section are as follows:

(A) Health claims or equivalent encounter information.
(B) Health claims attachments.
(C) Enrollment and disenrollment in a health plan.
(D) Eligibility for a health plan.
(E) Health care payment and remittance advice.
(F) Health plan premium payments.
(G) First report of injury.
(H) Health claim status.
(I) Referral certification and authorization.

[4] 42 U.S.C. § 1320d-1(c)(3)(B)(iii).

[5] Letter from Ed Jones, chairman, WEDI, to the Hon. Tommy G. Thompson, secretary of health and human services 1 (Apr. 15, 2003) (available at http://www.wedi.org/cmsUploads/pdfUpload/commentLetters/pub/Letter_to_Sec_Thompson_pdf.pdf) (hereinafter the ''WEDI letter'').

cessful implementation, given a substantial degree of noncompliance in October 2003, and thus avoid the so-called *train wreck* that will result from reversion to paper claims or stoppage of cash (payment) flows[?]''[6]

Similarly, on May 19, the American Hospital Association's chief Washington counsel wrote to the director of the Office of HIPAA Standards of the Centers for Medicare and Medicaid Services at HHS.[7] She expressed her association's concern this way: ''[T]he greatest concern . . . is the potential for disruption in the current claim submission and payment cycles that might result from poor, improper or incomplete implementation of the transactions standards. Maintaining proper cash flow is critical for all hospitals . . . . Even a slight decrease in claims processing volumes or lengthening of the payment cycle could negatively affect hospitals' ability to care for their patients.''[8]

The health insurance industry could also face dramatically increased costs. If providers are unable to send electronic claims because of an inability to comply perfectly with HIPAA transactions rules, those providers would have little choice but to send paper claims to commercial health insurance carriers, albeit at a significant sacrifice of cash flow. The cost for a commercial health insurance carrier to process an electronic claim is between 25 cents and 75 cents per claim, but the cost associated with processing paper claims is between $2 and $12 per claim.

If only a small percentage of providers reverted to submitting paper claims, health insurance carriers' additional processing costs could rise disastrously. The ramp-up to paper processing would require significant cash outlays from health insurers for temporary staff to handle the greater volume of paper claims. Further, processing paper claims is time-consuming and would lead to excessive delays in paying claims. This would probably result in large-scale violations of state prompt-payment laws, which in turn would trigger substantial penalties and interest payments for payers.

The stakes are high. Health care is the largest industrial sector in the U.S. economy.[9] The daily transaction volume for health care insurance claims—whatever the dollar figure—is enormous. The health care industry depends on successful processing of reimbursement claims and the resulting cash flow to stay in business and continue serving patients. A major disruption to this cash flow would have alarming consequences.

Why, so late in the process, is the U.S. health care industry facing any substantial doubt at all about whether the conversion to HIPAA standard transactions will succeed? Part of the problem arises from the tardiness of HHS in developing and publishing transactions standards and accompanying instructions that are sufficiently detailed for this massive conversion. Further, the current secretary of HHS has failed to devote the HHS resources required to publicize the transition, explain it to all sectors of the industry, and encourage the necessary redesign of health care business processes—all necessary for the transition to succeed. The result is that significant sectors of the health care system, such as small physicians' practices, do not yet fully appreciate the extent of the complexities that must be mastered before the Oct. 16 deadline, nor do they fully understand the business and regulatory ramifications of failing to adjust in time.

At the same time, many in the health care industry apparently have misjudged the complexities of the business process changes HIPAA demands. Providers must reprogram their computer systems to furnish the additional information necessary under the HIPAA transactions standards. Providers and payers also must realign their business practices to accommodate the new inputs and outputs for HIPAA transactions.

This sounds abstract, but it is very real. Providers who do not redesign their business processes now are unlikely to be able to submit electronic claims successfully under HIPAA in October.

The redesign of business processes, including relationships with trading partners, must be shaped in part by the legal framework for standard transactions. This framework includes the regulation of health insurance at both the federal and state level, as well as regulation of health care reimbursements. A hazy view of the law, and doubts about the legal underpinnings of standard transactions, no doubt contribute to the industry's fear and uncertainty about the transition.

Political blame surrounding the changeover to standard transactions may be debated over the coming months. However, predictions about political consequences are not the focus—and are beyond the scope—of this article. Instead, this analysis concentrates on legal and business complexities inherent in using HIPAA standard transactions. The aim is to highlight legal and operational issues with HIPAA transactions, and suggest ways to deal with them between now and the Oct. 16 deadline. In short, this is a roadmap to aid the transition to HIPAA standard transactions.

Health Care Reimbursements

HIPAA standard transactions address the process by which a patient obtains health insurance and later receives insurance payments for health care. HIPAA standard transactions take the patient (or the individual, such as a parent or spouse, who pays the patient's health care insurance premiums) through every step of the process. Standard transactions are used for enrolling in a health plan; verifying eligibility for insurance coverage when the patient appears at a doctor's office, clinic, hospital, or similar facility; and making a claim for insurance coverage after receiving treatment. They are also used when the insurance company adjudicates the claim, that is, when it determines whether an insurance payment is appropriate, and notifies the patient of the determination. Finally, they are used when actually making the payment, either by check or—HIPAA's ultimate vision—by electronic transfer.

If the payment is made by electronic deposit to the patient or to the provider (doctor, clinic, hospital) who gave the care, then the payment is an electronic funds transfer (EFT). Performing some or all these functions electronically , with minimal or no human intervention, is called electronic data interchange.

---

[6] *Id.* (emphasis in original).

[7] Letter from Melinda Reid Hatton, vice president and chief Washington counsel, American Hospital Association, to Jared Adair, director, Office of HIPAA Standards, Centers for Medicare and Medicaid Services 1 (May 19, 2003) (available at http://www.hospitalconnect.com/aha/key_issues/hipaa/content/letterjaredadair_transactionsandcodes.pdf) (hereinafter the ''AHA letter'').

[8] *Id.* at 1.

[9] *See* U.S. Department of Health and Human Services, *Health Care Financing Review, Statistical Supplement*, 1999, at 2.

  ECLR ISSN 1098-5190

Some transactions are designed in pairs. For example, a claim to the insurance company for reimbursement is followed by a return transaction, the insurance company's notification to the claimant of the outcome of claim adjudication, and, if appropriate, a payment (by check or EFT), with a corresponding notification of payment, called a ''remittance advice.''

Each transaction is given a number in HIPAA's nomenclature. These numbers are part of the code used by people involved in HIPAA when they discuss particular transactions. For example, a health care claim is referred to as an ''837.''[10] The return payment advice—or notification that reimbursement is paid or denied in whole or part—is spoken of as the ''835.''[11]

This article will concentrate on the 837/835 transaction pair (claim for payment/payment and remittance advice) because claims for payment, and the insurance companies' payments or denials of reimbursement, are the heart of the HIPAA transactions process. Moreover, if there is a disruption of cash flow on and after Oct. 16 it will come from the inability of insurance companies' computers to process 837 claims successfully and pay the claims via 835s. (The deficiency may or may not lie with the insurance companies' computers, but more of that later.)

These relationships are reflected in the three categories of HIPAA ''covered entities.'' They are (1) health care providers (*e.g.*, doctors, hospitals, therapists, laboratories) that electronically bill at least one HIPAA standard transaction, (2) health plans (health insurers), and (3) health care clearinghouses.[12]

By statutory definition, a health care clearinghouse does at least one of two things. It takes a transaction in nonstandard format and code and converts it to a HIPAA standard transaction, *i.e.*, one in the HIPAA-prescribed format and using the HIPAA-prescribed computer code.[13] This enables the clearinghouse to serve as a functional intermediary between, say, a doctor's office that lacks the computer capacity to generate standard transactions and the insurance company whose computers will (on and after Oct. 16) accept only standard transactions, *i.e.*, those using HIPAA standard format and standard code.[14]

Conversely, the clearinghouse may receive standard transactions from a health plan (the insurance company) and convert them into a nonstandard format so that various doctors' offices (or other providers), using their pre-HIPAA computer systems, can receive the insurance company's 835 remittance advices. Congress's inclusion of clearinghouses in the HIPAA statute explicitly recognizes that, by the deadline, significant parts of the health care industry will not have spent the time and money for new computer systems capable of EDI transactions using the HIPAA standard. Thus, clearinghouses are a safety valve.

The deadline is significant. The HHS secretary may impose civil penalties on covered entities for failure to use standard transactions after the deadline.[15] Moreover, HIPAA's criminal penalties[16] may apply to any ''person,''[17] among them HIPAA covered entities, who use nonstandard format and code sets to conduct what is defined under the statute and HIPAA rules as a standard transaction.[18] The reason is that these transactions contain protected health information (PHI) such as unique health identifiers and individually identifiable health information relating to a patient or other ''individual.''[19]

Short History of the October 2003 Deadline

Under the HIPAA statute as originally signed into law in 1996, the deadline to begin using HIPAA standard transactions was 24 months after the adoption date of the transactions standards (the date when HHS's order adopting the standards became effective).[20] The deadline date originally was Oct. 16, 2002. When it became obvious that meeting that deadline was infeasible, the industry sought, and Congress passed, the Administrative Simplification Compliance Act of 2001 (ASCA),[21] extending the deadline one year, to Oct. 16, 2003.[22]

Among other things, ''ASCA prohibits HHS from paying Medicare claims that are not submitted electronically after October 16, 2003,'' although the Secretary can grant waivers of this requirement.[23] Avoiding exclusion from Medicare is a powerful incentive for many providers.

Under ASCA, a covered entity seeking a delay of the transactions compliance deadline was required to file with HHS a request for extension.[24] As required in ASCA, the HHS request form included a statement that the covered entity had a plan for achieving compliance with the requirements for standard transactions by the new October 2003 deadline.[25] For example, the covered entity's compliance plan was required to include the start of testing HIPAA standard transactions by April 16, 2003, six months in advance of the October dead-

[10] *See* Health Insurance Reform: Standards for Electronic Transactions; Final Rule and Notice, 65 Fed. Reg. 50,312, 50,368 (Aug. 17, 2000) (codified at 45 C.F.R. pt. 160, Subpart A and pt. 162, Subpart I; *amended by* Health Insurance Reform: Modifications to Electronic Data Transactions Standards and Code Sets, 68 Fed. Reg. 8,381 (Feb. 20, 2003) (codified at 45 C.F.R. pt. 162) (collectively, the ''TCS Rules'').

[11] 65 Fed. Reg. at 50,368 (codified at 45 C.F.R. § 162.920(a)(viii)).

[12] 42 U.S.C § 1320d-1(a); 45 C.F.R. § 160.103 (definition of ''covered entity'').

[13] 45 C.F.R. § 160.103 (definition of ''health care clearinghouse'').

[14] *See* 42 U.S.C. § 1320d-4(a)(2)(B) (relationship of health plan to clearinghouse).

[15] 42 U.S.C. § 1320d-5.

[16] 42 U.S.C. § 1320d-6(b).

[17] 42 U.S.C. § 1320d-6 (a).

[18] *See* 42 U.S.C. § 1320d-6 (a)(1), (2), (3).

[19] To use these elements of PHI ''in violation of this part''—''Part C – Administrative Simplification'' of the HIPAA statute—probably is a HIPAA criminal offense.

The lowest level of criminal offense is a fine of not more than $50,000, imprisonment of not more than a year, or both. If a court were to determine that the use was for ''commercial advantage,'' the penalty could be a fine up to $250,000, imprisonment of up to 10 years, or both. 42 U.S.C. § 1320d-6 (b)(1),(3).

[20] 42 U.S.C. § 1320d-4(b)(1)(A).

[21] Administrative Simplification Compliance Act, Pub. L. 107-105, § 2 (Dec. 27, 2001), 115 Stat. 1003 (codified in part as note to 42 U.S.C.A. § 1320d-4 (hereinafter ''ASCA'')).

[22] *Id.* at (a)(1).

[23] *Id.* at (b)(1).

[24] *Id.* at (a)(2).

[25] *See* CMS Public Affairs Office, Press Release, *CMS Issues Model Plan to Extend Deadline for Compliance with Electronic Transactions Rule*, March 29, 2002 (available at http://aspe.os.dhhs.gov/admnsimp/PRelease.htm).

line.[26] Neither ASCA nor HHS specified what constituted ''testing'' for this purpose.

Throughout ASCA, Congress is specific about Oct. 16, 2003's being the statutory deadline for covered entities to use only standard transactions for EDI in health care. On or after the deadline, if a health care transaction is conducted electronically, and if it is functionally one of the transactions described in the HIPAA statute and HIPAA transaction and code set rules, then it must be conducted using the HIPAA rules' specified format and code set. Congress made no provision for the Secretary to extend the deadline; Congress expected the deadline to be firm. This conclusion is apparent from ASCA's structure and language.

Can the Deadline be Moved?

Now the health care industry is facing a deadline that appears too close to permit a satisfactory level of compliance. WEDI wrote in its letter to the HHS secretary that noncompliance in as little as five percent of claims (*i.e.*, insurance companies' rejection of more than five percent of the claims submitted daily or weekly) would have an adverse impact.[27] Among other things, claim rejections at this level or greater (rejection rates of fifty percent or more are being discussed informally at industry meetings attended by this author) could lead providers to revert to submitting claims on paper rather than electronically.[28]

This volume of paper claims would overwhelm health care insurers. Handling paper claims would require hiring and training staff to deal with claims that now are submitted using the insurance companies' proprietary systems—the very formats and codes outlawed as of Oct. 16. The reimbursement process would bog down immediately. Payments to providers would be slowed, perhaps by weeks or longer. Hospitals' and doctors' cash flow would diminish substantially. The disruption to providers' finances, and probably to patient care, would be significant.[29]

Anticipating a crisis, health care organizations are warning the secretary of a ''train wreck,''[30] and suggesting ways for the secretary to extend the deadline or otherwise avoid catastrophe.[31] What chance is there that these suggestions might succeed?

Some proponents assert that the secretary has inherent executive authority to extend the deadline, relying on the notion that an executive agency's decision not to exercise its enforcement powers is often unreviewable by courts, as discussed in *Heckler v. Chaney*.[32] This argument is unlikely to succeed for two reasons.

First, the HHS already has concluded that ''[the secretary has] no statutory authority to extend the compliance dates beyond this 1-year [ASCA] extension period.''[33]

Second, the presumption of agency discretion to refrain from using enforcement powers upheld in *Heckler v. Chaney* is confined by the odd facts of that case.[34] The statute in *Heckler* did not have a rigid structure, comparable to ASCA's, mandating enforcement of particular requirements by a set date. Indeed, the U.S. Supreme Court offered this admonition: ''We do not have in this case . . . . a situation where it could justifiably be found that the agency has 'consciously and expressly adopted a general policy' that is so extreme as to amount to an abdication of its statutory responsibilities. . . . Although we express no opinion on whether such decisions would be unreviewable . . . . We note that in those situations the statute conferring authority on the agency might indicate that such decisions were not 'committed to agency discretion.' ''[35]

If the secretary were to extend ASCA's deadline, he could do so only by abdicating his duty to enforce a deadline specified unambiguously by Congress. Even if his action were called an enforcement ''moratorium'' or a comparable term, it would in practice be an extension of the Oct. 16 deadline, and hence in violation of the statute.

If ultimately an extension really is the only answer to the dilemma posed by the impending mandated conversion to standard transactions, the remedy—extending an unrealistic deadline—lies only with Congress. The considerations in seeking an extension from Congress and the attendant political complications are beyond this article's scope.

The AHA suggests a different course. It proposes a ''system-wide implementation plan'' under which the Secretary would order insurance companies to make ''contingency payments'' to providers.[36] These payments would be required after a ''contingency triggering event,'' occurring when the insurance reimbursement payments to a provider dropped below five percent of a historical baseline of claims processed for the prior year.[37] (Other aspects of the AHA proposal, dealing with the processing of standard transaction claims, are discussed below.)

AHA's proposal on behalf of hospitals will predictably be opposed by, among others, health insurers. They are likely to argue that the secretary has no authority under HIPAA, ASCA, or any other statute to impose a requirement on health plans to make ''contingency payments'' based on ''contingency triggering events.'' Health insurers are likely to argue that mandated payments would be especially inappropriate when made to pay providers (hospitals, physicians, or others) whose electronic claims are rejected because they appear deficient.

No doubt health insurers will warn the secretary that, were he to try to adopt the AHA's suggested plan, his

[26] *See generally* Cassie M. Chew, *Experts Give Different Views on HIPAA Rule Delay*, 10 Health Care Policy Report, No. 1, 5 (2002); Peter Kongstvedt and Margie Lewis, *HIPAA: Now That There's a Delay. . . .* , 10 Health Care Policy Report, No. 4, 159 (2002).

[27] WEDI letter, Exhibit 1, at 1.

[28] *Id.*

[29] AHA letter at 1.

[30] WEDI letter at 1.

[31] *Id.*, Exhibit 1, at 2-4.

[32] 470 U.S. 821, 832 (1985).

[33] TCS Rules, 68 Fed. Reg. at 8,384.

[34] Federal district court denied relief to death row inmates who sought enforcement by the Food and Drug Administration against ''off-label'' use of drugs to administer lethal injections in prison executions. The U.S. Supreme Court held that the FDA's decision not to take enforcement action was not subject to review under the Administrative Procedure Act, because the presumption that agency decisions against using enforcement powers are unreviewable was not overcome by the enforcement provisions of the Food, Drug, and Cosmetic Act. *Heckler*, 470 U.S. at 833.

[35] *Id.*, n.4 (internal citations omitted).

[36] AHA letter, Attachment at 2-4.

[37] *Id.* at 3.

  ECLR ISSN 1098-5190

order (and the plan) could be challenged successfully in court. Events are unlikely to make a challenge necessary, because it should be apparent to the secretary that he would have no statutory basis—and no other ground—for requiring these kinds of payments from health insurers. HIPAA and ASCA may be combining with the realities of an extraordinarily complex, nationwide computer conversion to produce a ''train wreck,'' ''meltdown,'' or however else the problem is described; but the secretary cannot manufacture new remedies, unauthorized by statute, as a solution.

Sarbanes-Oxley Duties: Crisis in the Making?

Before and after the passage of ASCA, thoughtful people in the industry anticipated the business consequences of a disruption to health care reimbursements. Anecdotal evidence suggests that experienced executives, consultants, and other advisors believed that insurance companies would want to continue paying claims even if the claims did not meet HIPAA's transactions standards. They hypothesized that payers (insurance companies) would voluntarily pay claims that did not satisfy HIPAA, in order to avoid disrupting cash flow to providers.

All this was before passage of Sarbanes-Oxley.[38] A full discussion of Sarbanes-Oxley's impact on health care reimbursements is beyond the scope of this article. However, two considerations under Sarbanes-Oxley deserve discussion.

First, publicly traded providers, clearinghouses, and insurers must consider now how to evaluate predictions of a substantial adverse impact on health care reimbursements, and industry cash flow, as a result of recent developments such as the letters from WEDI and AHA. If a publicly traded provider, clearinghouse, or insurer concludes it might be materially affected by these potential adverse events, it must consider its new disclosure obligations. Doing so will necessarily include assessment of the risk of litigation arising from possible failures to submit or successfully process reimbursement claims.[39]

Second, publicly traded insurers must consider how they will deal with electronic claims (837s) that fail to pass their computer processing standards. As of October 16, 2003, it will be a potential civil and criminal violation to pay claims that apparently do not satisfy HIPAA's standards, as specified in the HIPAA transaction rules. Thus, the notion of paying claims whether or not they meet HIPAA standards is no longer an option. In all likelihood, corporate counsel will rule out any such course. This puts a premium on understanding when a submission is, in the jargon of the industry, a ''clean claim,'' *i.e.*, one that should, or must, be processed and paid.

HIPAA's Requirements for Standard Transactions

Part of the problem faced by the health care industry under HIPAA is uncertainty about the processing requirements for HIPAA standard transactions. Health care reimbursement transactions are complex because they must be able to deal with a wide variety of health problems and treatments; they must satisfy complex federal and state statutes and regulations governing reimbursement; and they must meet contractual requirements of particular health insurers before payment is proper. It is important to know how these complexities are dealt with in HIPAA standard transactions, and particularly in making claims (the 837 transaction) and adjudicating and paying them (the 835 remittance advice transaction).

Another way to ask this question is: what, exactly, must a claim be, or have, to comply with HIPAA? When dealing with HIPAA standard transactions, what is a ''clean claim''? What other requirements apply to the claim and its processing?

The standards for HIPAA transactions derive from three sources: the statute itself, HHS's rules implementing the statute, and implementation guides for each transaction. The statute contains an initial list of standard transactions.[40] The rules adopted by HHS describe the format for standard transactions generally and specifically for each transaction. The format specified generally is the ANSI X12N format developed by a private-sector body, the American National Standards Institute.[41]

There are particular code sets that are stated in the ANSI X12N format for each transaction. For example, for professional (as contrasted to institutional) provider claims (837s), the rules specify use of the ASC X12N 837 Version 4010.[42] To non-initiates, this is opaque. It is simply the specification of a particular set of computer code (printed, it is a thick document) that allows a provider to make claims with specificity.

These code sets are found or referenced in the implementation guide for each particular transaction. Each implementation guide, which in the HIPAA rules is an ''implementation specification,''[43] is listed in the rules themselves.[44]

These formats and code sets are not sufficiently detailed in themselves to permit HIPAA standard transactions. There must be additional detail added by the parties (for example, the claimant and the insurance company in a claim or 837 transaction, which produces a return remittance advice, or 835, from the payer insurance company). Then, the HIPAA transaction must be contained inside communications codes to enable electronic data interchange (much as a letter is mailed in an envelope).

These additional details typically are spelled out in agreements between the parties known as trading partner agreements.[45] The HIPAA rules anticipate trading partner agreements. They specify that trading partner agreements may not:

> (a) Change the definition, data condition, or use of a data element or segment in a standard.
>
> (b) Add any data elements or segments to the maximum defined data set.

---

[38] Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745 (2002).

[39] *See generally* Filing Guidance Related to Conditions for Use of Non-GAAP Financial Measures, 68 Fed. Reg. 15,939 (April 2, 2003).

[40] *See* U.S.C. § 1320d-2.

[41] TCS Rules, 45 C.F.R. § 160.103 (definition of ANSI).

[42] 45 C.F.R. § 162.920 (a)(1)(ii), § 162.1102(c).

[43] 45 C.F.R. § 160.103 (definition of ''implementation specification'').

[44] 45 C.F.R. § 162.920; §§ 162,1201-1802 (for each individual standard transaction).

[45] 45 C.F.R. § 160.103 (definition of ''trading partner agreement'').

> (c) Use any code or data elements that are either marked ''not used'' in the standard's implementation specification or are not in the standard's implementation specification(s).
>
> (d) Change the meaning or intent of the standard's implementation specification(s).[46]

The HIPAA rules also place limits on what a health plan may require in processing transactions. Among other things, ''[a] health plan may not reject a standard transaction on the basis that it contains data elements not needed or used by the health plan (for example, coordination of benefits information).''[47] The preamble to the transaction rules (published with the rules as part of the notice-and-comment rulemaking) explains further how health plans are to process these transactions. The Implementation Guides contain maximum data sets. When filing a claim, the provider uses those data elements that ''are relevant to the transaction and necessary to process it.'' In addition, the claim may include data elements that are ''situational,'' *i.e.*, necessary in some situations but not in others.[48]

The preamble anticipates that those submitting standard transactions will only send the minimum data elements necessary to process the transaction.[49] There should be a general understanding among covered entities that, when submitting a standard transaction, not all data elements listed in the relevant implementation guide need be used. Instead, only the minimum number of data elements should be submitted.

In reality, this understanding is not pervasive in the industry. The problem is spelled out in the addendum to the AHA letter:

> [I]t will be virtually impossible for a covered entity to be certain that [its] submission includes each of the required and situational elements that need to be present in every transaction it sends. This problem largely results from the ambiguity of ''situational'' data and how they are applied to various health plans. Frequently, the reporting of the situational[ly] defined data is specific to the type of service, the category of provider, and the different health plan benefit coverage requirements, just a few of the items that influence reporting variations. Almost inevitably data elements will be missing for many of the individual transactions. This is true even if every health plan and provider is prepared to process the standard *form* of each transaction (or use a clearinghouse . . .), *and* to use only the standard code sets required by the regulation. More importantly, it seems quite likely that health plans' HIPAA compliant systems may reject such transmissions as ''non-compliant.'' In fact, some systems reportedly will reject an entire batch of claims as ''non-compliant'' if one of the included claims is missing elements. The receipt of significant volumes of such rejection messages will inevitably cause the claims payment system to collapse.
>
> The problem for both the submitter and the health plan is that the *content* requirements established in the implementation specifications for each of the standard transactions in many, if not all [*sic*] cases, requires more data elements than is required to actually adjudicate the transactions.
>
> . . . .
>
> At the October compliance date and for some time thereafter, the potential for implementation failure be-

---

[46] 45 C.F.R. § 162.915.

[47] 45 C.F.R. § 162.925(a)(3).

[48] ''We wish to clarify the maximum defined data set concept. A maximum defined data set contains all of the required and situational data elements possible in a standard transaction. For each standard transaction there are situational data elements that are both relevant to the particular transaction and necessary to process it; there are also situational data elements that an entity may include in a transaction, but does not need to include, in order for the transaction to be processed. A required data element is always required in a transaction. A situational data element is dependent on the written condition in the implementation specification that describes under which circumstances it is to be provided. The maximum defined data set is based on the implementation guides and not the addendum in the proposed rule. The maximum defined data set also includes the applicable medical and nonmedical code sets for that transaction.'' *Health Insurance Reform: Standards for Electronic Transactions*, 65 Fed. Reg. 50,312, 50,322 (Aug. 17, 2000).

[49] ''We note that if an entity follows the implementation specification and the conditions in the implementation specification for each transaction, the entity will only be supplying the minimum amount of data elements necessary to process a transaction (required data elements and relevant situational data elements); the entity will not be supplying possible but unnecessary situational data elements. In addition, we note that the intent behind the maximum defined data set was to set a ceiling on the nature and number of data elements inherent to each standard transaction and to ensure that health plans did not reject a transaction because it contained information they did not want. For example, if an implementation specification defines a health care claim or equivalent encounter information transaction as having at most 50 specific data elements, a health plan could not require a health care provider to submit a health care claim or encounter transaction containing more than the 50 specific data elements as stipulated in the implementation guide. (A health plan may, however, request additional information through attachments.)'' *Id*. at 50322-23. Health plans also need to consider ramifications under HIPAA's privacy rule from requiring from providers more situational data than is necessary to adjudicate a claim. Requiring providers to submit excess situational data—for example, in a health plan's ''companion guide'' to HIPAA transactions—may cancel the general exclusion of standard transactions from HIPAA's minimum necessary rule. *See* 45 C.F.R. §§ 502(b), 514(d); *Standards for Privacy of Individually Identifiable Health Information; Final Rule*, 67 Fed. Reg. 53,182, 53,199 (2002): ''Except to the extent information is required or situationally required for a standard payment transaction (*see* 45 C.F.R. § 162.1601, 162.1602), the minimum necessary standard applies to a covered entity's disclosure of protected health information to a financial institution in order to process a payment transaction. With limited exceptions, the Privacy Rule does not allow a covered entity to substitute the judgment of a private, third party for its own assessment of the minimum necessary information for a disclosure. Under the exceptions in § 164.514(d)(3)(iii), a covered entity is permitted reasonably to rely on the request of another covered entity because, in this case, the requesting covered entity is itself subject to the minimum necessary standard and, therefore, required to limit its request to only that information that is reasonably necessary for the purpose.'' Thus, if a provider or clearinghouse is aware that a health plan is routinely asking for protected health information this is not mandatory or ''situationally required,'' and yet gives in to the health plan's demand (which may be in the plan's ''companion guide''), there is a privacy rule violation. Of course, if the health plan is aware that its companion guide is requiring the routine submission of protected health information that is neither mandatory nor situationally required to process claims, then the plan is willfully committing privacy violations. This potentially subjects those involved to civil and criminal penalties under 42 U.S.C. §§ 1320d-5 and 1320d-6(a). The criminal penalties may be applied both to individuals and organizations, *see* §§ 130d-2(a)(2)(c), 1320d-6(b).

  ECLR ISSN 1098-5190

> comes extraordinarily high . . . . Health plans may find themselves buried in paper claims, or find that each claim is submitted as a unique electronic transaction rather than as [part of] a batch . . . .
>
> Providers, on the other hand, may find that the submission of a claim believed to be in HIPAA standard format is rejected by the health plan for non-compliance because the provider's interpretation about whether to report a situational element is different from the payer's interpretation. It will be extremely costly to figure out which data element is missing if the plan does not provide feedback. Moreover, such delays will increase the potential for a disastrous impact on the provider's cash flow; consequently many providers will have little choice but to drop a resubmission to paper.[50]

For transactions, this lack of correspondence between the concept of HIPAA compliance as seen by submitters and processors—usually providers filing claims and payers (insurance companies)—is echoed in WEDI's letter: ''WEDI respectfully requests that the [s]ecretary provide guidance to the healthcare industry . . . on what is meant by the term 'compliance' . . . .''[51]

It makes sense to ask how these fundamental ambiguities could remain unresolved so late in the day, for a process authorized by statute in 1996, and having such a significant impact on the delivery of health care services in the United States. Presumably, basic elements of the standards for processing standard transactions should have been foreseen and resolved long ago by HHS, preferably in a notice-and-comment rulemaking.[52]

For whatever reason, HHS has not anticipated the need to furnish sufficient guidance on what obviously is an existing industry-wide point of confusion. If left unresolved, this issue appears ready to derail the Oct. 16 transition and create, in its wake, substantial disruption and hardship in the delivery of health care. What can the secretary do between now and Oct. 16 to fix the problem?

Notice-and-comment rulemaking, even if conducted on an emergency basis, would still take weeks (significant because fewer than 20 weeks remain to the deadline). Any solutions proposed by the Secretary must be understood by the health care industry (and its computer system vendors) well enough to be coded into software, distributed and installed on thousand of computer systems, and tested end-to-end between trading partners (providers and payers) and their clearinghouses.[53] There is not enough time remaining between now and the deadline to accomplish all this, even assuming the secretary had an answer to the dilemma outlined so carefully by AHA and WEDI.

There is concern that payers would violate the HIPAA statute and rules if they accepted for processing anything less than a perfect transaction, with every field filled precisely as the implementation guide mandates, and no matter what the difference in interpretation of the implementation guide between the submitter and the receiver (in an 837 claim, for example, between the provider and the insurance company).[54] Of course, consistently producing perfect electronic claims in the 837 format, and in high volume, is exceedingly difficult. It surely is not a fact of commercial life before the October 2003 deadline. Nevertheless, there seems to be a widespread belief that HIPAA requires providers to submit, and payers to pay, only on the basis of perfect claims. Analysis of all applicable law demonstrates that this belief is wrong, and that the combination of commercial and regulatory problems in handling standard transactions – while formidable – are not beyond solution.

Without precluding the possibility of the secretary's action to help in the transition, what is there in existing law and other guidance that may ameliorate the problem?

First, nothing in the HIPAA transaction rules specifies what is meant by a ''HIPAA-compliant'' claim or other transaction. One searches the rules in vain for that guidance. It may be surprising that the question is not addressed, either in the text of the rules or in the explanatory preamble, but it is not.

Rather, the HIPAA transaction and code set rules require electronic transactions that are functionally described in the transaction regulations to use HIPAA-prescribed standard formats.[55] Consequently, ANSI X12 formats are required, and other formats (for example, NSF, a format in commercial use at present) do not satisfy the rules.

However, there is no requirement that HIPAA standard transactions must be devoid of errors, on pain of the submitters' being subject to penalties. Indeed, the implementation guides contemplate errors and describe how to deal with them. For example, the implementation guide for the 270/271 transaction pair states: ''If data is missing or invalid, it must be corrected and a new transaction must be generated.''[56]

The task for a payer is to be able to identify errors via software, generate reports detailing those errors, and transmit the information back to the submitter so that the transactions, with errors corrected, can be resubmitted. Software and hardware is commercially available that will perform these tasks, even at the high volumes of transactions that payers must handle. Conse-

---

[50] AHA letter, Attachment at 1-2.

[51] WEDI letter at 2.

[52] Using notice-and-comment rulemaking, rather than a less formal process for so important a part of the standard transactions process, is vital. Formal rulemaking, or some other process with the formality required by case law, avoids the uncertainty arising from informal administrative pronouncements such as answers to FAQs (frequently asked questions), which do not bind the agency and are unlikely to be given deference in the courts. *See United States v. Mead Corp.*, 533 U.S. 218, 227 (2001); *see also Chevron U.S.A. Inc. v. Echazabal*, 122 S.Ct. 2045, 2048 (2002); *Edelman v. Lynchburg College*, 122 S.Ct. 1145, 1150 (2002).

[53] AHA emphasizes the importance of end-to-end testing. AHA letter at 2.

[54] ''[W]e have heard from some providers concerned that their fiscal intermediaries have indicated that, for batched transactions where a single claim within the batch contains an error, the entire transaction batch will be returned without processing rather than just the individual deficient claim. Processing claims in such a way is inefficient and costly and only guarantees significant disruptions in the claims processing and payment cycles. Returning only deficient claims, while processing the rest of the transaction [*sic*] that are part of the batch is the more efficient and less disruptive approach.'' AHA letter at 3.

[55] *See* 45 C.F.R. § 162.920; §§ 162.1201-1802.

[56] ASC X12N Insurance Subcommittee Implementation Guide, Health Care Eligibility Benefit Inquiry and Response: 270/271 at 23 (May 2000).

quently, expecting trading partners to accommodate these functions is commercially reasonable.

One can envision HIPAA 837 claims, in standard transaction formats, that have errors. Some errors may be material, because the payer needs particular data elements to be correctly represented in order to adjudicate and pay the claim. Other errors may be insubstantial. Some data elements prescribed in the 837 Implementation Guide (which has the force of law under the transaction rules because it is prescribed for use in the transaction rules)[57] may not need to be used at all by the payer, because the payer does not need those particular data to adjudicate the claim or to determine how, where, and to whom to make payment. In other words, those data elements are not needed for a ''clean claim.''

Importance of What Is Not Preempted

What law applies to the question of how payers must proceed with claim processing under these circumstances? What law dictates to the trading partners (the provider and the payer in an 837 claim-835 remittance advice, for example) how the claim is to be processed, when the payer may or must accept the claim, and when the payer may or must reject the claim (and what the payer may or must do if the claim is rejected)?

The statute itself is the place to begin this inquiry. Congress specified rules for HIPAA's preemption of state law.[58] For preemption to occur, a state law must be ''contrary'' to the statute or the rules adopted by HHS to implement it. This protocol is amplified in rules adopted by the secretary.[59] Among other things, these rules delineate when a state law is ''contrary'' to the statute or HIPAA regulations: when a covered entity would find it impossible to comply with both the state and federal requirements, or if state law is an obstacle to accomplishing the full purposes and objectives of the statute.[60]

Because a standard transaction is an insurance claim or other transaction related to insurance, it is, in the absence of preemption by HIPAA, governed by state contract law, with emphasis on the state law of insurance contracts.[61] State (and federal) consumer protection and state (and federal) unfair competition laws also come into play.[62]

The threshold question in preemption analysis is whether these state laws are ''contrary'' to HIPAA. The answer may eventually come in litigation, but it is likely to be ''no.'' State laws regulating insurance[63] and protecting consumers of insurance products and services are natural adjuncts to HIPAA. They support HIPAA's goals, rather than conflicting with federal requirements or with HIPAA's purposes and objectives.

In other words, state law regulating health insurance is complementary to HIPAA. It is therefore not preempted, and is enforced alongside HIPAA's statutory and regulatory requirements.

Analyses of HIPAA to date appear to have missed this basic relationship. HHS has not issued guidance emphasizing this essential legal connection. Yet many of the questions asked throughout the health care industry about how insurance companies should, or must, process claims and other transactions are answered, not by HIPAA or other federal law, but by state laws.

The exception may be Medicare and Medicaid, operated by the Centers for Medicare and Medicaid Services, a part of HHS and the nation's largest health insurer and payer. CMS is not subject to state insurance regulation, and so in theory could adopt a commercially unreasonable, and ultimately politically self-defeating, policy of insisting on perfection in the submission of claims. Because a commercially reasonable approach to claims processing is in everyone's interest, including CMS's, there is hope that CMS might soon adopt, announce, and emphasize in instructions to its fiscal intermediaries and submitters commercially reasonable claims processing protocols that mirror those of payers that are subject to state insurance regulation.

Speaking generally, these laws require that consumers of insurance products and services be treated fairly, in a commercially reasonable way. Again speaking generally, hyper-technical rejections of health care claims because of mistakes in providers' filling out the data fields of HIPAA standard transactions would not be viewed by the courts, or by state insurance regulators, as commercially reasonable. Rather, they might be viewed as unfair or deceptive trade practices. Delays in payments to providers or insureds for unwarranted rejection of HIPAA standard transactions (without giving the submitter details of the errors and an opportunity to cure them) would likely be regarded as violations of state prompt-payment laws, unless the payer could demonstrate mitigating circumstances under those laws.

If the transactions were true electronic data interchange payment transactions, UCC Article 4A (electronic funds transfer) would also apply. Article 4A has been adopted by all the states and as well by the Federal Reserve system, so it is pervasive.[64]

Article 4A specifically requires commercial reasonableness in the security measures that parties to a funds transfer must use. More generally, Article 4A is structured to adapt legal requirements to the realities of technology in commercial computing environments. There, mistakes, if not common, are still a routine occurrence that the funds transfer system must handle efficiently in practice. Article 4A's provisions deal with

[57] 45 C.F.R. § 162.1102.
[58] 42 U.S.C. § 1320d-7.
[59] 45 C.F.R. § 160.201-205.
[60] 45 C.F.R. § 160.202 (definition of ''contrary'').
[61] *See generally*, 1 COUCH ON INSURANCE 3d § 1.46 (1997).
[62] *Id.* at §§ 4.18-4.25.
[63] *Cf. Kentucky Association of Health Plans Inc. v. Miller*, 123 S. Ct. 1471 (Apr. 2, 2003) (holding that provisions of a state law regulating insurance were not preempted by ERISA).

[64] *See* 12 C.F.R. § 210.25(b); *see also* 12 C.F.R. § 210.25(c). ''The [Federal Reserve] Board's Regulation J, subpart B, which incorporates Article 4A of the Uniform Commercial Code, and Operating Circular 6 (Funds Transfers through Fedwire), issued in accordance with Regulation J, govern Fedwire funds transfers. Under Regulation J and Operating Circular 6, the Federal Reserve Banks can also impose conditions on an institution's use of Fedwire. In particular, Operating Circular 6 requires each Fedwire participant to enter into a security procedures agreement with its Federal Reserve Bank.'' FEDERAL RESERVE BOARD, *Fedwire Funds Transfer System* (Dec. 19, 2001) (available at http://www.federalreserve.gov/paymentsystems/coreprinciples/) (footnote omitted).

The Federal Reserve Board's Regulation E will apply to electronic funds transfers as part of HIPAA standard transactions involving financial institutions and consumers (insureds, patients) as defined in the regulation. Regulation E's purpose is the protection of consumers engaging in electronic funds transfers. 12 C.F.R. § 205.1 *et seq*.

  ECLR ISSN 1098-5190

mistakes organically through protocols that are legally enforceable. Through the imposition of commercially reasonable protocols, Article 4A reflects an accommodation to the inevitable problems encountered in moving payment orders electronically. Therefore, even though Article 4A does not demand in terms that participants in funds transfers behave with commercial reasonableness (except for the security measures they use), its architecture imposes a regime of commercial reasonableness.

Participants in the HIPAA funds transfer system must be flexible enough to deal with common mistakes, know how to correct them, and accept certain mistakes that, for one reason or another, are not, or cannot feasibly be, corrected. Courts may by analogy extend Article 4A's commercially reasonable structural approach to the conduct of other HIPAA standard transactions that may not, strictly speaking, involve EDI transfers (for example, eligibility inquiries). The other HIPAA standard transactions are closely related to HIPAA claim and payment transactions in the health care business cycle. Therefore, analogous structural principles may be appropriate, especially in the larger framework of state contract and consumer protection laws and state insurance regulation.

Trading Partner Protocols

In this framework, trading partners—providers and payers—are under a duty to agree on business processes that embody commercial reasonableness. They should devise business processes to enable payers to identify

(1) whether transactions are in HIPAA standard format,

(2) whether some transactions have errors,

(3) which transactions have errors that are immaterial to adjudication and payment, and so can be processed, *i.e.*, the errors are insignificant, and

(4) which transactions have errors that are material, so that they are barriers to adjudication and payment, and require that the errors be corrected before the claim can be processed, *i.e.*, the errors are significant. This can be done largely by computerized means.

Present practice in much of the industry might suggest that incomplete, incorrect, or otherwise imperfect claims are typically rejected by some payers even in situations where the error is obvious to the payer or of little consequence to the validity of the underlying claim. In fact, that is not the case. Today, generally more than 95 percent of all electronic claims submitted are accepted by payers. That is, today, providers generate the information that payers need to adjudicate claims more than 95 percent of the time.

The payer requirements for adjudication generally should not be any different because providers are submitting claims using HIPAA standard transactions. Both before and after Oct. 16, 2003, payers must have rules about which transactions they will accept, reject, place in pending status, or work with the provider to fix.

In other words, HIPAA does not mandate a change in this overall set of industry patterns. All else being equal after Oct. 16, 2003, a payer should not have a higher rejection rate with HIPAA standard claims transactions than with the pre-HIPAA formats currently being used. It should be permissible under existing state contract law for a pair of trading partners—provider (or clearinghouse) and payer—to agree to commercially reasonable processing arrangements (with keen attention to HIPAA's rules preventing modification of standard formats and codes[65]). The trading partners also must give due regard to prompt payment and other consumer protection laws, which themselves are a reaction to strict processing rules that became obstacles to fair treatment of health care claimants.

The implementation guides acknowledge and promote the fundamental necessity of trading partner agreements. Here is a typical explanation:

> It is appropriate and prudent for payers to have trading partner agreements that go with the standard Implementation Guides. This is because there are two levels of scrutiny that all electronic transactions must go through.
>
> First is standards compliance. These requirements MUST be completely described in the Implementation Guides for the standards, and NOT modified by specific trading partners.
>
> Second is the specific processing, or adjudication, of the transactions in each trading partner's individual system. Since this will vary from site to site (e.g., payer to payer), additional documentation. . .will prove helpful to each site's trading partners (e.g., providers), and will simplify implementation.
>
> These types of companion documents should exist solely for the purpose of clarification, and should not be required for acceptance of a transaction as valid.[66]

Thus, so-called payer-specific ''companion guides'' must not require anything that contravenes the content specified in the implementation guides, or in the HIPAA transactions rules themselves. This still leaves room for payers to require certain data (e.g., contract numbering) that do not contravene the implementation guides.

The instructions in the implementation guide for the 837 institutional claim transaction offer guidance about the role of trading partner agreements (the same instructions are found as well in implementation guides for the other standard transactions):

> These standards do not define the method in which interchange partners should establish the required electronic media communication link, nor the hardware and translation software requirements to exchange EDI data. Each trading partner must provide these specific requirements separately.
>
> . . . .
>
> With a few exceptions, this implementation guide does not contain payer-specific instructions. Trading partners agreements are not allowed to set data specifications that conflict with the HIPAA implementations . . . . However, . . . [t]he payer, acting in accordance with policy and contractual agreements, can ignore data within the 837 data set. In light of this, it is permissible for trading partners to specify a subset of an implementation guide as data they are able to *process* or act upon most efficiently . . . . Thus, it behooves trading partners to be clear about the specific data within the 837 (i.e., a subset of the HIPAA implementation guide data) they require or would prefer to have in order to efficiently adjudicate a claim. The subset implementation guide must not contain any loops, segments, elements or codes that are not included in

[65] 45 C.F.R. § 162.915.

[66] ASC X12N Insurance Subcommittee Implementation Guide, Health Care Eligibility Benefit Inquiry and Response: 270/271, 10 (May 2000).

the HIPAA implementation guide. In addition, the order of data must not be changed.[67]

As a practical matter, the transition to the new standardized transaction formats necessitates cooperation throughout the industry between payers and providers. The aim of cooperation should be to process large volumes of transactions successfully—so that claims are adjudicated and paid on a timely basis—under HIPAA's new regime. A widespread inability to process standard transactions, and maintain throughput, serves no one's interests.

Between now and the transition, the industry is served by creating an environment where providers and payers can cooperate in accommodating existing industry patterns of dealing with the efficient processing of new standard transaction formats and codes.[68]

The transition demands that payers and providers cooperate to figure out how commercial reasonableness can guide their relationships without creating commercial disadvantages to either the payer or provider communities. After all, neither is served if there is a significant disruption to the health care payment system when the deadline arrives. Everyone wants to keep their customers happy. Payers also have a substantial interest in forestalling the wrath of state insurance regulators. That group is likely to play a decisive role if there is a HIPAA-induced breakdown of health care reimbursements come October, accompanied by charges that payers are rejecting clean claims.

The obligation to pay claims arises from underlying insurance contracts. Denying reimbursement of a clean claim invites a private lawsuit under state law for breach of the insurance contract. If reimbursement of clean claims is denied or improperly delayed on a systemic basis, payers invite class action lawsuits on state law theories including breach of contract and bad faith.

There is an urgent need for legally sound, workable business process redesign to accommodate HIPAA transactions. How might industry-wide accommodation work? The preferred approach—and probably the only workable one, despite its transaction costs—is to embody the agreements about business process in trading partner agreements.

Where the parties' agreed-upon business processes (presumably built around computerized transaction analysis and reporting systems) identify transactions in HIPAA standard format and code but containing significant errors, the parties should use technological means agreed upon in advance in their trading partner contract to notify the provider (or other sender) of the errors, so that they can be corrected and the transactions resubmitted for processing. There will be extraordinary effort and expense required industry-wide to devise the right forms for trading partner agreements, negotiate them, and implement them in business processes and computer code before Oct. 16. However, that cost is preferable to payers' being buried in paper claims by providers who, in turn, are stymied by HIPAA's requirements for electronic claim submission.

Trading partner agreements should also cover use of testing protocols in advance of the compliance deadline.[69] Reliance on trading partner agreements may be more cumbersome and far more expensive than current practice in many parts of the health care sector. However, in light of HIPAA's security requirements as well as the confusion surrounding the transaction rules, trading partner agreements are more advisable than ever before – indeed, as a practical matter to satisfy HIPAA's security requirements,[70] they are all but mandatory. The standard of care required of a covered entity under the statute and security rules makes it presumptively imprudent to exchange protected health information for billing purposes unless and until the parties can point to a trading partner agreement or an equivalent protocol that specifies how the exchanges will be kept secure according to HIPAA's high standards.

A Role for Health Care Industry Trade Groups

In summary, the unattainable goal of having to produce perfect HIPAA-standard claims is not a HIPAA requirement. The whole idea of ''perfect-or-else'' is contrary to applicable state law on which HIPAA relies to complete the regulatory framework for transactions processing.

State contract, insurance regulation, consumer protection, and unfair competition law dovetail with HIPAA to produce a commercially reasonable approach to health care transaction processing. The HIPAA transaction rules require that standard transactions be in HIPAA-prescribed formats and use HIPAA-prescribed code sets. They do not require that use of these formats be error-free before processing can occur.

Implementation of ''commercial reasonableness'' in transaction processing is feasible because commercial software vendors now offer products that can report on transaction errors in detail, and in the high volume that the industry must handle daily. Payers and clearinghouses need this capability in order to perform the consultation with providers that is essential to the real-world processing of claims.

Industry groups could perform a great service if they were to develop ''protocols of cooperation'' to guide providers and payers in structuring their HIPAA trading partner relationships. They could facilitate the transition to standard transactions by suggesting common checklists for drafting and negotiating HIPAA trading partner agreements. The protocols—suggestions only—might jump-start trading partner negotiations. Protocols of cooperation would also have significant value in educating the industry about elements of business process development for dealing with standard transactions.

As part of this road-map, industry groups could explain the legal underpinnings of HIPAA as it combines with state law to create a commercially reasonable framework for handling standard transactions. Some

[67] ASC X12N Insurance Subcommittee Implementation Guide, Health Claim: Institutional: 837 12-13 (May 2000).

[68] This is the approach taken by the State of New Jersey. Department of Banking and Insurance, Office of the Commissioner, *Memorandum to NAIC Commissioners' Round Table*, undated (available at http://www.wedi.org/cmsUploads/pdfUpload/commentLetters/pub/Hanks3-0331NJ-NAIC1.pdf).

[69] *See* AHA letter at 2 (discussing the importance of end-to-end testing).

[70] Statutory security requirements are found in 42 U.S.C. § 1320d-2(d)(2); regulatory implementation of the statutory requirements is found in 45 C.F.R. § 164.530(c) (privacy rules) and Part 164, Subpart E (security rules); *see Health Insurance Reform: Security Standards; Final Rule*, 68 Fed. Reg. 8,334 (Feb. 20, 2003).

  ECLR ISSN 1098-5190

industry groups might even investigate sponsoring an expedited process for mediating disputes between providers and payers who are having difficulty negotiating their trading partner relationships, or who are having disputes about how to continue and to document existing relationships through the transition.

There is also an important role in this process for the National Association of Insurance Commissioners[71] and individual state insurance commissioners. They administer the insurance regulatory regimes that will combine with HHS's TCS rules to shape the health care transactions process in October. NAIC, following the lead, for example, of the State of New Jersey,[72]can work with HHS and health care industry groups in fashioning protocols of cooperation to guide the rapid development and negotiation of workable, legally appropriate trading partner agreements.

With this kind of direction, the industry may make substantial progress on standard transactions before the October deadline. Even so, however, the prospect of significant disruptions to cash flow as a result of difficulty in meeting HIPAA requirements will remain up to the deadline and, unfortunately, for some time afterwards.

For this reason, we can expect to see hospitals, physicians' practices, and other providers undertake financial contingency planning to deal with anticipated disruptions to their cash flow. These efforts may include negotiating with willing payers (who are concerned with the satisfaction of their base of insurance customers) for interim payments at predetermined levels, pending determination of claims after processing problems are resolved. This interim might last days or weeks.

Financial contingency planning also may include arranging bank lines of credit to sustain providers through the transitional period of diminished cash flow. Providers with strong credit and good banking relationships, and who seek these arrangements early, may find the process little more than routine. Less creditworthy providers, or those who start their financial contingency planning closer to the October deadline, may find the going rougher. It will be interesting to see how banks nationwide react to the prospect of substantial credit demands around the deadline.

A key to the success for all industry efforts is public support from the secretary of HHS for the guiding *state law* principle of commercial reasonableness in payers' processing of HIPAA transactions. HHS should offer formal and informal guidance to the health care industry about how HIPAA and the state law of insurance regulation, contracts, and electronic funds transfer play together in the legal framework for transactions processing. Without that official instruction from HHS, the industry is unlikely to pull together effectively—assiduously negotiating trading partner agreements and selecting the necessary software systems to analyze claims—to get through the October transition without substantial pain.

---

[71] http://www.naic.org

[72] *See supra* n.68.