HIPAA SECURITY
Compliance Insider

A PLAIN-ENGLISH GUIDE TO HIPAA SECURITY & TCS REGULATIONS

AUGUST 2003

IN FUTURE ISSUES

- Create Software Inventory for Disaster Recovery and Patch Management
- Tips for Protecting Live Test Data
- List of Key Web Sites for Finding Out Your Security Vulnerabilities

How to Conduct a HIPAA Security Risk Analysis

One of the first things the HIPAA security regulations require you to do is perform a security risk analysis to identify and evaluate the vulnerabilities and threats to your organization's electronic protected health information (EPHI). "Conducting a security risk analysis is essential," says information security expert Harry Smith. "You won't know what security measures to implement until you know what risks you face from threats to your EPHI."

A thorough risk analysis is important for much more than HIPAA compliance. It gives security professionals a helpful document that they can discuss with the organization's executives for security budgeting and planning purposes. But many security professionals we talked to don't know where to begin in conducting a risk analysis. Part of the problem, says Smith, is that the HIPAA security regulations don't give you a checklist of things to consider.

We'll tell you what a risk analysis is and how to conduct one. We'll also give you two Model Forms you can choose from to conduct your own security risk analysis (see p. 3).

What's a Security Risk Analysis?

According to HIPAA's security regulations, a security risk analysis is a thorough assessment of the potential risks to the confidentiality, availability, and integrity of your organization's EPHI. In a risk analysis, you identify all of the vulnerabilities of your EPHI and the threats that can occur because of those vulnerabilities. Then you calculate the effect of each threat on your EPHI if it were to actually occur, explains risk analysis expert Thomas C. Peltier. If threats create too great a risk to your EPHI, you must then look for safeguards and countermeasures that will lessen the threats and mitigate the damage they might cause.

Select from Two Approaches

According to Peltier, there are as many different styles and types of risk analysis as there are organizations trying to run them. But there are two basic approaches to conducting a risk analysis: quantitative and qualitative. Both approaches are well accepted. Our Model Form I follows the quantitative approach; Model Form II follows the qualitative approach. Use whichever form best suits your organization's needs.

Quantitative. This approach requires you to assign a numerical value to the probability that a particular threat will occur to your EPHI and the likely loss should that threat occur. You must use numbers and formulas to determine the dollar value of each loss on an annual basis, says health information security attorney M. Peter Adler.

(continued on p. 2)

Editor: **Amy E. Watkins, Esq.**
Executive Editors: **David B. Klein, Esq., Nicole R. Lefton, Esq., Susan R. Lipp, Esq., Janet Ray**
Senior Editors: **Nancy Asquith, Heather Ogilvie**
Copy Editors: **Cynthia Gately, Graeme McLean**
Proofreader: **Lorna Drake**
Production Director: **Mary V. Lopez**
Senior Production Associate: **Sidney Short**
Production Associate: **Jennifer Chen**
Director of Planning: **Glenn S. Demby, Esq.**
New Projects Editor: **Rebecca L. Margulies, Esq.**
Dir. of Ref./Information Development: **John D. Boyd**
Marketing Director: **Peter Stowe**
Associate Marketing Director: **Ellen Teatsorth**
Director, List Services: **Denise M. Fisher**
Marketing Mgrs.: **Christine Chan, Michael F. Sherman, Stephen Sullivan**
Data Processing Manager: **Rochelle Boorstein**
Sales Manager: **Joyce Lembo**
Customer Service Reps.: **B. Maslansky, H. Therezo**
Director of Operations: **Michael Koplin**
Fulfillment Supervisor: **Edgar A. Pinzón**
Financial Manager: **Janet Urbina**
Asst. Office Manager: **Maria Safina**
Publisher: **George H. Schaeffer, Esq.**
Owners: **Andrew O. Shapiro, Esq., John M. Striker, Esq.**

Subscriptions: *HIPAA Security Compliance Insider* is published monthly. Subscription rate: $297 for 12 monthly issues. Address all correspondence to: Brownstone Publishers, Inc., 149 Fifth Ave., New York, NY 10010-6801. Tel.: 1-800-643-8095 or (212) 473-8200; fax: (212) 473-8786; e-mail: awatkins@brownstone.com

Disclaimer: This publication provides general coverage of its subject area. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional advice or services. If legal advice or other expert assistance is required, the services of a competent professional should be sought. The publisher shall not be responsible for any damages resulting from any error, inaccuracy, or omission contained in this publication.

HIPAA SECURITY RISK ANALYSIS (continued from p. 1)

Determining each threat's annual loss expectancy is very helpful because it allows you to compare actual dollar values of the loss to the cost of the safeguard that will reduce or mitigate that loss, says Adler. So, for example, if you determined that the annual loss expectancy to a computer from power surges might be $2,000, spending $20 for a surge protector and $400 a year to back up EPHI every night would probably be worthwhile.

Qualitative. Qualitative risk assessments don't require you to place a precise numerical value on the probability of a threat or effect of an anticipated loss. Instead, you identify risks—and the likelihood that they'll occur—on a scale ranging from high to low. The purpose of a qualitative risk analysis is to prioritize the various risk elements in subjective terms, says Peltier. You would also have to determine the highest numerical risk level your organization would accept.

So if you determine that the total risk level to EPHI on the computer from a power surge exceeds the risk level your organization is willing to accept, you'll have to find ways to reduce that risk.

Which Risk Analysis Approach Is Better?

Neither approach to risk analysis is better than the other, says Peltier—they both have good points and bad. A qualitative risk analysis is relatively simple, he says, requiring few calculations. But he warns that it's very subjective and the results depend entirely on the quality of the risk management team you've assembled.

There are also pros and cons to performing a quantitative risk analysis. It gives you a much more workable cost/benefit analysis, says Adler. But it's labor intensive and requires extensive research on asset valuation and threat probability. And a quantitative risk analysis still contains some measure of subjectivity, he adds.

HIPAA's security regulations don't require or even show a preference for either approach, says Adler. So you can perform whichever one works better for your organization.

SIX STEPS FOR EVERY RISK ANALYSIS

Whether your risk analysis is quantitative or qualitative, experts agree that it should include the following six steps:

1) Identify Assets

You need to know what assets you're trying to protect before you can protect them, says Smith. "When you're starting a risk analysis, the very first step must be to understand where your risk comes from," he explains. "If you don't do that, nothing else will make sense." This is essential, whether you're doing a quantitative or qualitative risk analysis.

Everything you have that stores or transmits EPHI is an asset for which a risk analysis should be conducted. Each of our Model Forms includes two examples of assets—a network server and MRI equipment [Forms I & II, col. 1]. With Peltier's help, we've also given you a list of the most common assets containing EPHI (see p. 4). But you should conduct a complete inventory of your organization and its systems to identify where your EPHI comes from, where it's stored, where it goes, and who has access to it along the way.

Get additional information for quantitative risk analysis. If you're performing a quantitative risk analysis, you'll also need to calculate what each asset is worth, says Adler. So, for instance, we've given a value of $80,000 to the MRI example in our Model Forms [Form I, col. 1].

Placing a value on each physical asset isn't that difficult—you can use standard asset valuation processes, such as fair market value or replacement cost. The best place to start may be your financial statements.

But you have to add the value of EPHI to the value of each asset. Placing a quantitative value on EPHI, which is one of a health care organization's greatest assets, can be very difficult. It's easy to say that each computer is worth about $2,000, but how do you know how much your patient's medical chart is worth? Adler suggests that you derive this

(continued on p. 4)

MODEL FORMS

Choose Qualitative or Quantitative Risk Analysis

Below are two forms you can choose from to perform a risk analysis—one form should be used when performing a qualitative risk analysis and the other form should be used when performing a quantitative risk analysis. Both forms require you to list each of your organization's assets that contains electronic protected health information (EPHI). Each form also requires you to identify the threats and vulnerabilities to those assets and the safeguards and countermeasures available to combat those threats and vulnerabilities.

The quantitative risk analysis form (Form I) requires you to assign actual values to your assets and the harm that each threat would cause to your asset. Then you determine the probability of each threat's occurrence to establish the amount that each threat is expected to cost your organization each year.

The qualitative risk analysis form (Form II) requires you to assign a number on a scale of 0–5 (with 0 being the lowest) to the likelihood of each threat's occurrence. You must assign another number (also on a scale of 0–5) to the anticipated severity of the threat's impact to your EPHI. Multiplying those numbers will give you a total risk level that can range anywhere from 0 to 25. This total risk level will help you prioritize your security tasks.

We've included examples on the first two lines of each form to help you get started.

I: QUANTITATIVE RISK ANALYSIS

1 Asset/ Total Value	2 Vulnerability/ Threat	3 Exposure Factor (% of Loss if Threat Occurs)	4 Single Loss Expectancy (Col. 3 x Value in Col. 1)	5 Annualized Rate of Occurrence (Estimated Frequency of Expected Threat)	6 Annualized Loss Expectancy (Col. 4 x Col. 5)	7 Safeguards/Countermeasures & Annualized Cost
Network Server $500,000	Accessible via Internet/hacker	80%	$400,000	Once a week (52/1)	$20,800,000	1. Firewall ($50,000/year) 2. Intrusion Detection System ($200,000/year) 3. Encryption ($200,000/year)
MRI Equipment ($80,000)	Accessible to public/theft	100%	$80,000	Once in 10 yrs. (1/10)	$8,000	1. Encryption ($20,000/year) 2. Locks ($500/year) 3. Bolt Equipment to Floor ($500/year)

II: QUALITATIVE RISK ANALYSIS

1 Asset	2 Vulnerability/ Threat	3 Impact to EPHI (Scale of 0–5, 0=No Impact)	4 Likelihood of Occurrence (Scale of 0–5, 0=No Likelihood)	5 Total Risk Level (Col. 3 x Col. 4)	6 Safeguards/ Countermeasures
Network Server	Accessible via Internet/hacker	5	5	25	1. Firewall 2. Intrusion Detection System 3. Encryption
MRI Equipment	Accessible to public/theft	5	1	5	1. Encryption 2. Locks on Equipment 3. Bolt Equipment to Floor

HIPAA SECURITY RISK ANALYSIS

(continued from p. 3)

value much the same way a dollar value is assigned to intellectual property. Although this analysis will partly include qualitative methods, you can also consider the potential fines and other costs associated with a HIPAA violation or a lawsuit over a breach of confidentiality.

***Insider* Says:** Putting together a list of assets for the first time can be time-consuming. Try starting with asset lists your organization has already created for financial statements and privacy compliance efforts. Once you finish your list, be sure to continually update it and perform a new risk assessment for each item that you add, says Smith.

2) Identify Vulnerabilities and Threats

For each asset you identify, list each vulnerability and threat that can harm that asset and the EPHI it contains. Vulnerabilities are different from threats, cautions Smith. A vulnerability is a system defect or flaw—something that's inherent in the asset. A threat is something that exploits that vulnerability. For example, a significant vulnerability associated with wireless networks is the broadcast of EPHI through the air for anyone with a wireless card to pick up. The threat is that someone without authorization will intercept it and alter, sell, or destroy it.

Identifying each vulnerability will help you determine what threats you need to prevent or mitigate. Some vulnerabilities can pose more than one threat. In our MRI example in the Model Forms, we identified the equipment's accessibility as a vulnerability that could lead to the threat of theft [Forms I & II, col. 2]. But public accessibility could also allow the MRI to be damaged, either from accidents or vandalism. Below, there's a list of common vulnerabilities and threats, prepared with Peltier's assistance.

3) Assess Severity of Threat

For each asset, consider how each threat you've identified affects the confidentiality, integrity, and availability of EPHI, says Adler. Take MRI equipment for example. If it's stolen, will the thief be able to get access to the EPHI? Aside from the damage resulting from the loss of EPHI to your organization, what damage would occur if the thief divulged the EPHI to a third party, such as the press? The way that you record the severity of the threat depends on whether you're performing a qualitative or quantitative risk analysis.

Quantitative risk analysis. If you're performing a quantitative risk analysis, determining the threat's severity is a two-part process:

- First, determine the actual loss to your asset and EPHI caused by the threat—that's called the "exposure factor." In our MRI example on the form, the exposure factor for the theft of an MRI is 100 percent—that is, all of the value of the equipment and the EPHI on it would be lost [Form I, col. 3].

▶ *Three Lists to Help You Conduct Risk Analysis*

Here are lists that you can use as a starting point when conducting a risk analysis. They give examples of common assets containing EPHI, typical vulnerabilities and threats to those assets, and available safeguards and countermeasures to prevent or mitigate those vulnerabilities and threats. Each list is based on examples provided by Thomas C. Peltier and published in his book, *Information Security Risk Analysis* (ISBN 0-8493-0880-1), available at www.amazon.com.

These examples should help you get started on your organization's risk analysis. Some threats (such as a fire or flood) might be applicable to almost all of your organization's assets, while others (like theft or hacking) may apply only to certain assets. Conduct your own research to determine what's appropriate for your organization.

ASSETS

- ▶ **Network:** computers; medical equipment; front-end processors; workstations; modems; communication lines; data encryption tools; internal and external connectivity; remote access security.
- ▶ **Software:** operating systems; utilities; compilers; database software; application software; catalogued procedure libraries.
- ▶ **Physical:** building; heating, ventilation, and air-conditioning; furniture; supplies; machinery; fire control systems; data storage locations; modes of data transit.
- ▶ **Other:** employees; patients/customers; patient/customer records and information; procedures; patient/customer confidence.

VULNERABILITIES/THREATS

Fire; flood; natural disasters (including electrical storm, earthquake, snow, ice, tornado, volcanic disruption, and hurricane); chemical spill; denial of service; theft; alteration of data or software; bomb threat; unauthorized access; unauthorized disclosure; computer virus; power outage; operator or user error; hardware failure; software failure; telecommunications outage; employee strike.

SAFEGUARDS/COUNTERMEASURES

Employee policies and procedures (including sanctions); employee training; access restrictions, passwords, and other authentication measures; firewalls; intrusion detection systems; antivirus software; encryption; surge protectors; sprinklers; locks and intruder alarms; audit logs; backup copies; remote access.

■ Next, use the exposure factor to determine the effect of a single threat occurrence—called the "single loss expectancy"—for each asset and EPHI. Do this by multiplying the total value of your asset and EPHI ($500,000 for the MRI) by the exposure factor (100 percent). The result ($500,000) is the cost a single occurrence of the threat would have to your organization [Form I, col. 4].

Qualitative risk analysis. In a qualitative risk analysis, you would determine the severity of each threat to the asset and EPHI—its "impact"—on a scale ranging from low to high. Our Model Form uses a range from 0–5, with 0 meaning no impact. In the MRI example on the form, that impact would be very high—say, 5—because the organization would lose the equipment and all of the EPHI on it, and the thief could divulge the information to anyone [Form II, col. 3].

4) Determine Threat's Likelihood

Next, you'll need to determine the likelihood of occurrence for each threat. Again, how you do this depends on whether you are performing a qualitative or quantitative risk analysis:

Quantitative risk analysis. For a quantitative risk analysis, determine the "annualized rate of occurrence"—that is, how often that threat is likely to occur each year. In the MRI example, that might involve the use of theft averages compiled by local insurance companies to determine that without additional safeguards, MRI equipment might be stolen once every 10 years. So the annual rate of occurrence would be a fraction—1/10 [Form I, col 5].

Qualitative risk analysis. For a qualitative risk analysis, assign a relative value to the likelihood that a threat will occur. In our example, the theft of MRI equipment isn't very likely, so you might assign it a 1 (using the same 0–5 scale) [Form II, col. 4]. But other threats to the MRI—such as a power surge or water damage—may be more likely and would receive a higher number.

5) Calculate Annualized Loss/Total Risk Level

Finally, calculate the actual level of risk or annual expected loss that this particular threat poses to this asset.

Quantitative risk analysis. If you're conducting a quantitative risk analysis, you must calculate the "annualized loss expectancy"—the amount your organization should expect to lose or spend each year if the threat actually occurs. Do this by multiplying the single loss expectancy for each asset (Form I, col. 4) by the annualized rate of occurrence (Form I, col. 5). In our MRI example, the organization could expect to lose $8,000 each year ($80,000 x 1/10) if EPHI is lost or divulged because of the theft of an MRI, provided that additional countermeasures and safeguards aren't put in place to protect EPHI [Form I, col. 6].

Qualitative risk analysis. For a qualitative risk analysis, determine the total risk level by simply multiplying the impact to EPHI (Form II, col. 3) by the likelihood of the threat's occurrence (Form II, col. 4). This will give you the extent of risk that each threat poses to each asset on a scale of 0 to 25 with 25 being the greatest risk. In our MRI example, the risk to EPHI caused by theft of the MRI is a 5 (5 impact x 1 likelihood)—not very high [Form II, col. 5]. But if your organization has determined that it will not accept any risk over level 3, it will have to find a way to reduce this risk.

***Insider* Says:** A key way to identify threats and vulnerabilities is to conduct a thorough security assessment, says Adler. He suggests that you review your current technical, administrative, and physical security practices and conduct your own penetration testing—attempting to circumvent your organization's security measures as a hacker or thief would. There are a number of resources available if you decide to conduct a security assessment on your own. Two free ones online are:

■ Phoenix Health System's HIPAA Gap Assessment/Risk Analysis (www.hipaadvisory.com/action/compliance/gapassessment.htm); and

■ NIST's Security Self-Assessment Guide for IT Systems: (http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf).

6) Identify Safeguards/ Countermeasures

Finally, list possible safeguards and countermeasures for each vulnerability and threat you identified in step 2. You should list both the safeguards that you're already employing, as well as others that are available to you, says Peltier. For example, to guard against the risks associated with allowing access to MRI equipment, the examples on our forms list encryption, locks, and bolting the equipment to the floor [Form I, col. 7; Form II, col. 6].

We've provided examples of safeguards and countermeasures (see p. 4) to get you started. You may also want to talk to a security consultant to see what she recommends. Or you can research various Web sites, such as www.sans.org and www.searchsecurity.com, for descriptions and reviews of different types of safeguards and countermeasures to common vulnerabilities and threats.

(continued on p. 6)

HIPAA SECURITY RISK ANALYSIS

(continued from p. 5)

Quantitative risk analysis. If you're performing a quantitative risk analysis, you'll need to know the cost of each safeguard and countermeasure so you can compare it to the expense associated with the risk itself. For example, if you expect that a loss will cost $100,000 annually but the annual cost of the countermeasure is $500,000, the countermeasure probably isn't worth it.

Qualitative risk analysis. A qualitative risk analysis doesn't require calculations of costs and expenses, so you don't need to include the costs of safeguards and countermeasures on the qualitative risk analysis chart. But you'll probably still need to know how much each safeguard and countermeasure costs, says Smith, especially if you're forwarding the results of your risk analysis to management for budgeting purposes.

Impossible to Eliminate Risk

You'll never be able to get rid of all your risk connected to an asset unless you eliminate the asset from your inventory, warns Peltier. For example, one vulnerability associated with using a handheld device, such as a PDA, is loss or theft of EPHI. You can't eliminate the threat of someone's stealing a PDA unless you stop using it altogether. But you can reduce the threat by having policies and procedures that require employees to lock up PDAs. And if you've performed regular backups and encrypted EPHI so that only authenticated users can access it, you've mitigated the damage if a PDA is stolen. Your only loss will be the dollar value of the equipment, not the confidentiality or availability of EPHI. ■

Insider Sources

M. Peter Adler, Esq., LLM, CISSP: Partner, Foley & Lardner, 3000 K St. NW, Ste. 500, Washington, DC 20007-5101; padler@foley-law.com.

Thomas R. Peltier, CISSP, CISM: President, Peltier and Assocs., 13748 Fort St., Ste. 211, Southgate, MI 48195; trpeltier@peltierassociates.com.

Harry Smith, CISSP: Vice President of Product Development, PrivaPlan Assocs., Inc., 10300 W. 23rd Ave., Lakewood, CO 80215; hsmith@privaplan.com.

IN THE NEWS

▶ *California Law Requires Notification of Security Breaches*

A new California law requires every person or organization that conducts business in that state to notify state residents about any security breach that resulted in (or is reasonably believed to have resulted in) the unauthorized acquisition of that resident's unencrypted personal information. This notification must occur "in the most expedient time possible and without unreasonable delay." The new law, which went into effect July 1, 2003, also allows California residents who have been injured by a violation of the law to sue the individuals or organizations responsible.

California is the first state to enact this type of law, but experts agree that other states are likely to enact similar laws in the near future. A similar bill requiring notification of security breaches was introduced in Congress on June 26, 2003.

How Does This Law Affect You?

If you do business in California, every security breach to your system could trigger the law's notification requirement, provided that the following three criteria are met:

1) Personal information was (or is reasonably believed to have been) acquired by an unauthorized person. Unlike HIPAA, the California law only considers the actual acquisition (or reasonable belief of acquisition) of personal information by an unauthorized person to be a security breach. "Personal information" isn't public information—the law defines it as an individual's first name or initial combined with last name and any of the following:

- Social Security number;
- Driver's license number or California Identification Card number; or
- Account number or credit/debit card number with the security code, access code, or password that would permit access to an individual's financial account.

2) The security breach involved a California resident's personal information. It doesn't matter if the breach occurred in California or New York or elsewhere. As long as a California resident's personal information is affected, you'll have to notify that resident of the breach.

3) The personal information was unencrypted. If you encrypt the personal information of your California patients and customers, the law doesn't require you to notify them of any security breaches, even if the information was acquired by an unauthorized person.

***Insider* Says:** You can access the new California law by going to www.privacyprotection.ca.gov/laws.htm and scrolling down to "Notice of Security Breach—Civil Code Sections 1798.29 and 1798.82–84." ■

TRAPS TO AVOID

Don't Let Overload of Audit Trail Data Lead to Liability

The HIPAA security regulations require health care organizations to have mechanisms to monitor the activity in information systems containing or using electronic protected health information (EPHI). To comply with this requirement, organizations must generate "audit trails"—that is, data recording the activities information system users engaged in while they had access to systems containing EPHI. But the security regulations don't spell out exactly what data an audit trail must capture. They merely say that each organization must provide for an audit trail that's reasonable and appropriate based on its own needs and risk assessment.

On the theory that it's safer to include too much rather than too little data, some organizations implement audit trails that record each and every use of information systems containing or using EPHI. But this approach can actually *increase* your organization's liability risks.

Problem: Extensive Audit Trails Are Too Hard to Review

The problem is that simply generating audit trails isn't enough to comply with the HIPAA security regulations. You're also expected to review all of the audit trail data to determine if users engaged in any improper activity. But the more data your audit trails capture, the harder it is to review everything.

For example, suppose an organization authorizes physicians to access the medical records only of patients they treat. An audit trail shows that a physician viewed the file of a patient she wasn't treating. The physician might have had a legitimate reason to do this. To comply with the HIPAA security regulations, the organization would have to look into the matter—for example, by asking the physician's department head for an explanation. The organization may then have to take disciplinary action if it determines that the physician acted improperly.

This review is essential, explains health information attorney Jay B. Silverman. If an audit trail captures a potentially improper access and you don't notice it, you're at serious risk. "It's like a smoking gun," says Silverman. "Government investigators and plaintiffs' attorneys will be able to use your failure to notice a violation captured in your own audit trails as evidence of negligence and lax security."

"Audit trails that capture all accesses to systems containing EPHI will result in information overload," warns HIT consultant Tom Hanks. They'll report literally thousands of uses, the vast majority of which will be perfectly legitimate. "It will take a small army to go through all this data to find the improper uses," Hanks adds.

Solution: Use Audit Trails that Capture 'Exception Reports'

To avoid this problem, you need to make sure your audit trail captures only as much data as you're capable of reviewing. To do this, Hanks recommends that organizations use audit trails that capture only the potentially problematic uses and ignore the routine ones. This is called "exception reporting" because a use is captured only if it involves accesses outside the usual parameters. Because it cuts down dramatically on the data captured, exception reporting makes the review of audit trails a manageable task.

Example: A hospital has a policy that allows billing clerks access to patients' addresses and phone numbers, but not their diagnoses. Under exception reporting, audit trails would report only when billing clerks accessed information systems/files containing patient diagnoses. But accesses by clerks to information systems/files containing just patient addresses and phone numbers wouldn't be reported.

Other unusual or nonroutine uses that you may want to trigger an exception report could include:

■ Uses that occur when a user is off-duty, on vacation, or on a leave of absence;

■ Uses that occur while a user is simultaneously logged on to another location;

■ Accesses by physicians to records outside their specialty; and

■ Accesses by medical staff to the records of patients not under their treatment or patients they haven't treated or aren't expected to treat for at least 30 days.

***Insider* Says:** Remember that such uses aren't necessarily improper. They're just uses you'll want to look into. ■

Insider Sources

Tom Hanks: Director Integration Solutions, Health Care Practice, PricewaterhouseCoopers LLP, One N. Wacker Dr., Chicago, IL 60606; (312) 298-4228; Tom.Hanks@us.pwcglobal.com; www.pwcglobal.com/healthcare.

Jay B. Silverman, Esq.: Ruskin Moscou Faltischek, PC, 190 EAB Plz., E. Tower, 15th Fl., Uniondale, NY 11556-0190; (516) 663-6606; jsilverman@rmfpc.com.

TCS

How to Test Your Electronic Transactions for Compliance

If you filed a request to extend the deadline for compliance with the transactions and code sets (TCS) standards, you promised the government that you would be in "testing mode" no later than April 16, 2003. That means you should already be testing your electronic transactions to make sure that they're HIPAA compliant, says Larry Watkins, vice president of Claredi, a HIPAA testing and certification service. But recent surveys show that many providers haven't started this testing.

"Worse yet, many providers don't even know what it means to test, and the law doesn't define it," says Watkins. For example, do all transactions need testing, or only claims? How many claims should be tested? Using actual patient data? And tested with whom—payors, a clearinghouse, or a third-party testing service?

If these questions are on your mind, too, here's a look at what transactions you should be testing and how to do it. And we'll give you three steps to get you through the testing process and on your way to compliance with the TCS standards.

What Transactions Should You Test?

The TCS standards don't say what transactions you should be testing now, nor do they tell you how to do it. So your best bet is to test each of your transaction types in the order of their importance to your organization. "Understandably, providers will want to start testing with their claims," says TCS expert Robert Tennant. "If you don't get paid, that's more important than if you can't check eligibility electronically." But eventually, you must test compliance with *all* the electronic transactions standards that apply to your organization, such as claim status, remittance, and referrals, he emphasizes.

Here's a list of electronic transactions that might be relevant to your organization and that you should consider testing.

- ASC X12N 837–Health care claim and coordination of benefits (transmitted by provider);
- ASC X12N 270–Health care eligibility benefit inquiry (transmitted by provider);
- ASC X12N 271–Health care eligibility benefit response (transmitted by payor);
- ASC X12N 276–Health care claim status request (transmitted by provider);
- ASC X12N 277–Health care claim status response (transmitted by payor);
- ASC X12N 278–Health care referral certification and authorization (transmitted by provider); and
- ASC X12N 835–Health care claim payment/advice (transmitted by payor).

Why Should You Test?

According to Tennant, you should test each transaction format to determine if:

- The field lengths and placement within each transaction are correct. Each type of transaction has specific data requirements. If your data exceeds the length allowed by the transaction form or isn't in the right place on the form, the transaction will be rejected.
- You're capturing and transmitting all data required for each type of transaction. When you submit an electronic claim form, you'll have to include all of the necessary information about your visit with the patient. If you don't, your claim will be rejected.

***Insider* Says:** Use actual patient data—known as "live data"—when you test. Many providers think that they must use simulated information for testing a claim or other transaction, but that's not true, says Watkins. You should use live data to test your transactions because that's the best way to see if you're capturing the right information.

How Should You Test?

Follow these three steps to test your transactions:

1) Use certified vendor. If you want your electronic claims to get paid after Oct. 16, 2003, they must be HIPAA compliant. But you can't submit a HIPAA-compliant claim unless your billing software is HIPAA ready, says HIPAA consultant Rachel Foerster. For example, in the electronic claims forms required by the TCS standards, you must input a special relationship code depending on whether your patient is the stepson, foster child, or grandchild of the insured. If your software can't capture these codes, your claims won't be HIPAA compliant, says Foerster.

One way to make sure you're using HIPAA-ready software is to choose a software vendor that's been certified by a reputable independent testing service, says Watkins. Certification is important because it lets you know that the vendor's software has the capacity to capture all of the information required by the TCS standards and generate a HIPAA-compliant claim, Watkins explains. Ask your vendor if it has been certified and by which service.

***Insider* Says:** Don't think you can just rely on a software vendor's certification, warn Watkins and Foerster. Certification doesn't mean that all of the claims that you submit using that vendor's software *will be* HIPAA compliant. It just means that the vendor's software *is capable* of producing a HIPAA-compliant claim. But if the claim form is missing important information—say, treatment date or service provided—that claim won't be HIPAA compliant and won't get paid. Follow the next two steps, too, to help make sure you're capturing all of the information required on the claim form.

2) Use objective testing service. Before you send any electronic transactions to your payors, it's a good idea to contact an objective third-party testing service—such as Claredi, Edifecs, or Foresight. Have it put you on its testing schedule so you can test the transactions first to see if they comply with HIPAA's TCS standards. These services charge a fee based on the size of your organization and the number of transactions you're testing. But their expertise will save you the time and expense of figuring out why your transactions are being rejected. They'll tell you why your claims will be rejected before they actually are, says Watkins, so you can fix the problems before it's time to submit an actual claim to your payor.

You can send any number of each type of transaction to a testing service and it will tell you if the transaction is HIPAA compliant, says Watkins. But expect the worst. "We're not finding anyone who's HIPAA compliant the first time around," says Watkins. In some cases, the testing service's results might show that the provider forgot to capture important patient information. In others, the billing program may not have been formatted properly—so the claim won't contain all of the information required for that specialty or payor. "A testing service will work with you to fix these problems before you go any further," says Watkins. You may also need to work with your software vendor to understand your particular problems and get them addressed, he adds.

If you normally submit your own transactions to each payor, you can work with the testing service yourself. Or if you submit your transactions through a software vendor or clearinghouse, have it set up a testing schedule with the testing service for you. Even if you work with the testing service yourself, says Watkins, your vendor or clearinghouse can still help you if the transaction has problems.

***Insider* Says:** Many providers skip this step and go right to step 3—testing with individual payors. But that's not a good idea, warns Watkins. Testing your transactions with an individual payor won't tell you whether all of your claims will get paid. Even with the standardization required by HIPAA, different payors have different requirements that they list in their companion guides, says Tennant. For example, some payors, like Medicaid, require each claim to have the provider's taxonomy code—others don't. And not all payors are offering to test each type of transaction—many won't have this capability until well after the compliance deadline, says Tennant.

A good third-party tester will pull together the companion guide for each payor and compare your transactions to each one, so you'll know if your transactions meet the requirements of every one of your payors before you submit them. Whatever testing service you use, be sure to ask if it will test your transactions against the requirements in each of your payors' companion guides.

3) Test with individual payors. Finally, you'll have to submit sample transactions to each of your payors to check that they don't get rejected. To do this, call each payor and say that you're ready to test your transactions, just as you did with the testing service.

"Payors have testing schedules too, but they're much more crowded than an independent testing service's schedule, so you won't get much time to work with them if there's something wrong with your transactions," says Watkins. That's why it's good to use a testing service beforehand, agrees Tennant. If you've done that, testing with your payor should go quickly and smoothly, and you'll know that your claims will get paid. ■

Insider Sources

Rachel Foerster: CEO, Principal, Rachel Foerster & Assocs., Ltd., 39432 North Ave., Beach Park, IL 60099; rachel@rfa-edi.com.

Robert Tennant, MA: Senior Policy Advisor, Health Informatics, MGMA Health Care Consulting Group, 1717 Pennsylvania Ave. NW, Ste. 600, Washington, DC 20006; rmt@mgma.com.

Larry Watkins: Executive Vice President, Claredi Corp., 498 North 900 West, Ste. 120, Kaysville, UT 84037; larry.watkins@claredi.com.

DOS & DON'TS

✓ Tell Users How to Protect 'Strong Passwords'

If you require users to use "strong passwords," make sure you also show them how to protect those passwords. For example, warn them not to tell their password to friends or family and not to write it on a Post-it to stick on their PCs.

Many health care organizations require their users to use strong passwords to access information systems that store or use electronic protected health information (EPHI). Strong passwords are hard to crack because they don't use words and proper names as their root—instead, they generally combine alphanumeric and special characters into long strings capable of resisting dictionary attacks.

But "even strong passwords can be compromised if users fail to keep them secret," warns HIT consultant Miriam J. Paramore. Plus, the HIPAA security regulations require a health care organization to implement a security training and awareness program for members of its workforce, including information systems users. So educating your users about the importance of protecting passwords and training them how to do it should be part of this required program.

✗ Don't Use 'Live Data' to Market Software or Equipment

If your organization markets software and equipment to other organizations, make sure this software and equipment doesn't contain "live data," says HIPAA consultant Gwen Hughes. Live data, which is information taken from actual patient or member records, is electronic protected health information (EPHI), Hughes warns. If you use it without a proper authorization to show others how your software or equipment works, you'll very likely be in violation of both the HIPAA security regulations and the privacy regulations, she says.

Even changing a few fields—such as patient or member name or identifier number—isn't good enough, she warns. "Someone watching your demonstration may be able to identify the patient from the information you didn't change. If you knowingly use live patient data to market your software or equipment, you may be subject to significant fines and penalties under HIPAA." And you could be in violation of state privacy laws as well.

Just recently, the Hospice Patients Alliance reported that it filed a HIPAA complaint against a Florida hospice whose subsidiary developed and marketed record-keeping software using live patient data. According to the president of the Hospice Patients Alliance, the hospice's subsidiary released protected health information (PHI) from hundreds of patient records—including names, diagnoses, and Social Security numbers—to other hospices all over the United States. In some circumstances, patient names had been changed, but much of the information was identical to that in actual patient records. ■

Insider Sources

Gwen Hughes, RHIA, CHP: Business Development Consultant, Care Communications, 205 W. Wacker Dr., Ste. 1900, Chicago, IL 60606-1214; ghughes@care-communications.com.

Miriam J. Paramore: President & CEO, PCI: E-Commerce for Healthcare, 9001 Shelbyville Rd., ITRC Bldg., Louisville, KY 40222. (502) 429-8555; www.hipaasurvival.com.